职业教育教学用书

网络设备配置技术一体化教程

主　审　周碧旋

主　编　陈外平　彭　锦
余　波　杨剑涛

副主编　史硕江　吴玉锋
李永娜　张　凌

電子工業出版社

Publishing House of Electronics Industry

北京・BEIJING

内 容 简 介

本书在编写思想上，贯彻基于工作过程的课程理念，以“项目式教学”为主要思想，建立以项目为核心，以工作过程为导向，以真实的工作任务驱动为机制的教学过程；针对现实项目网络工程所需要的网络配置与管理中所涉及的各种网络技术；在内容的安排上，充分体现了先进性、科学性与实用性，引入企业真实的工程案例，按照实际的工作过程安排知识点。全书共分 7 个项目：家庭网络配置与管理、商畅数码有限公司网络配置与管理、富华酒店网络配置与管理、校园网络的配置与管理、碧宏电子有限公司网络配置与管理（ACL）、新锐集团公司网络配置与管理、工业园区网络配置与管理。本书每个项目后有相应的认证测试题供学生课后复习巩固。

本书可作为职业院校计算机网络技术及相关专业的教材，也可作为网络管理员、网络工程技术人员和网络爱好者的参考书。

图书在版编目（CIP）数据

网络设备配置技术一体化教程 / 陈外平等主编. —北京：电子工业出版社，2014.8
职业教育教学用书

ISBN 978-7-121-20857-7

Ⅰ. ①网… Ⅱ. ①陈… Ⅲ. ①计算机网络—高等学校—教材 Ⅳ. ①TP393

中国版本图书馆 CIP 数据核字（2013）第 145281 号

策划编辑：施玉新
责任编辑：郝黎明
印　　刷：
装　　订：
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×1 092　1/16　印张：11　字数：281.6 千字
版　　次：2014 年 8 月第 1 版
印　　次：2014 年 8 月第 1 次印刷
定　　价：24.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

在当今信息化社会中生活的各个方面都能见到网络技术的身影，它正在改变着人们的生活和思维方式。掌握网络设备配置技术是网络工程师必备的技能要求。虽然目前网络设备配置的教材很多，但真正能够以真实项目把理论知识融合到项目实践教程中的教材并不多见。编者本着“理论知识够用，强化专业技能”的原则编写此书，以适应职业院校学生以培养技能为主的目标。

本书立足于基于工作过程的计算机网络技术专业课程体系，按照计算机网络技术专业的培养目标和网络工程师的岗位职业能力要求进行编写。全书通过七个不同规模、不同行业背景的项目，并按照由小到大、由易到难的方式组织网络设备配置技术的知识点。这七个项目分别是：家庭网络配置与管理、商畅数码有限公司网络配置与管理、富华酒店网络配置与管理、校园网络的配置与管理、碧宏电子有限公司网络配置与管理（ACL）、新锐集团公司网络配置与管理、工业园区网络配置与管理。本书具有以下特点：

（1）知识点以项目引领，任务驱动的形式组织。每一个工作任务都有相关的背景知识与相应的实施过程操作步骤，并将知识点融入工作任务中，使读者学习起来简单明了、通俗易懂，从而能提高读者的学习兴趣。

（2）以理论知识够用、强化专业技能为原则。以培养组网、用网与管网能力为重点，将教材内容与职业培养目标相结合，强化学生的技能训练，在训练中巩固所学知识，力求理论知识简洁、实用。可为从事系统集成、网络工程实施与网络管理打下良好的基础。

（3）以项目为核心，以工作过程为导向，以工作任务为驱动的一体化教材。以企业真实项目背景引入工作任务，在完成工作任务的过程中学习理论知识和专业技能，真正做到了理论知识与实际操作有机结合。

本书由广东省技师学院、惠州市商贸旅游高级职业技术学校、柳州市第一职业技术学校和玉溪第二职业高级中学的陈外平、彭锦、余波、杨剑涛、吴玉峰、史硕江、张凌、李永娜、张文武、张焕明、李明、刘敏、李光寿、王志平、沈海亮、姚正刚、熊玉金老师共同编写完成，周碧旋主审。在此感谢神州数码网络有限公司和星网锐捷网络有限公司为本书的编写提供了许多帮助、指导意见和参考资料。感谢对本书编写过程中给予大力支持和帮助的院校及各界同仁。对编写过程中参阅大量的重要文献资料难以完全准确注明，在此深表诚挚谢意！

由于编著时间比较仓促，编者水平有限，书中难免存在不妥之处，敬请海涵见谅！并欢迎提出宝贵意见和建议。

编　者

目　　录

项目一　家庭网络配置与管理

项目背景

张先生一家有四口人，家里原来只有一台电脑，最近因为儿子、女儿的学习需要，张先生为他们各添加了一台计算机。现在需要把家里的 3 台计算机连接起来，组建家庭网络环境，实现共享文件信息，并且实现所有计算机都可以连接因特网。另外张先生新买了一台智能手机，希望在家里安装一个无线网络，实现手机无线上网。

家庭网络如图 1-1 所示。

图 1-1　家庭网络

项目分析

分析一：张先生希望把家里的 3 台计算机组成一个局域网，实现连接因特网。

分析二：张先生希望在家里安装无线网络，实现手机无线上网。

项目方案

家庭局域网结构简单，可采用星形拓扑结构，张先生家庭目前只有 3 台计算机，可选用四口的路由器；为满足移动设备无线上网，则需要购买带有四口家庭无线路由器，通过设置路由器 PPPOE 拨号实现宽带网的共享，开启路由器的无线开关，并设置相应的无线密码实现移动设备的安全上网，如图 1-2 所示：

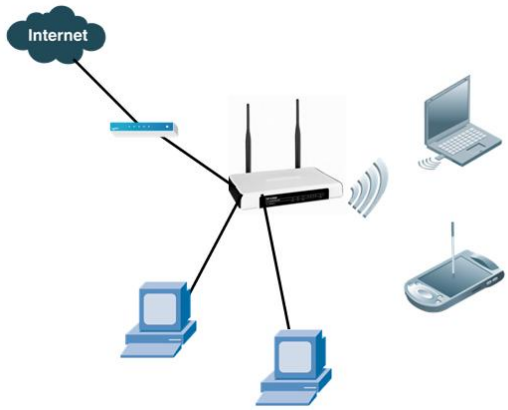


图 1-2　网络拓扑图

知识准备

1．家庭网络概述

1）家庭网络拓扑结构

随着宽带网正在迅速普及，并且一些家庭已经拥有 2 台以上的计算机，因此在家中组建小型局域网已成了一种适应发展的需要。一般来讲，作为一个家庭网络，接入的计算机数量很少，而且由于房间较小，布线长度较短，常用星形网络拓扑结构。星形拓扑结构是通过一个中心结点连接，这个中心结点为控制结点，任意两个结点的通信都必须通过它。这种拓扑结构通常使用集线器（HUB）或交换机作为中心设备，连接多台计算机，如图 1-3 所示

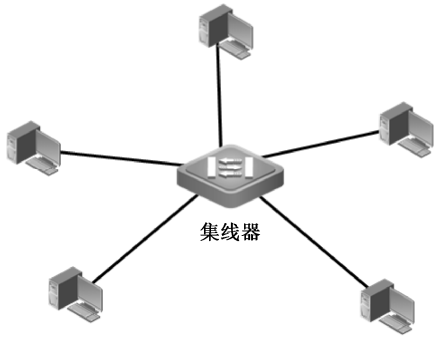


图 1-3　星形拓扑结构

2）网络设备选择

组建一个家庭网络，可能用到的设备器材有：网卡、网线、RJ-45 插头（水晶头）、集线器或者交换机、家庭路由器等。

（1）网卡

要组建一个家庭网络，所有的计算机必须要有网卡，网卡是计算机与外界局域网的连接是通过主机箱内插入一块网络接口板。网络接口板又称为通信适配器或网络适配器（network adapter）或网络接口卡 NIC（Network Interface Card）现在更多的人愿意使用更为简单的名称“网卡”。

网卡是工作在链路层的网络组件，是局域网中连接计算机和传输介质的接口，不仅能实现与局域网传输介质之间的物理连接和电信号匹配，还涉及帧的发送与接收、帧的封装与拆封、介质访问控制、数据的编码与解码以及数据缓存的功能等。常见的 RJ-45 型接口网卡如图 1-4 所示。USB 无线网卡如图 1-5 所示。

图 1-4　常见的 RJ-45 型接口网卡

图 1-5　USB 无线网卡

（2）网络线缆的选用

在局域网目前的传输介质中，有同轴电缆、双绞线和光纤可供我们选择，同轴电缆技术较旧，且安装困难，早已被市场淘汰，光纤介质传输信息快捷、损耗微小、防干扰能力强，但是由于其本身及相关配件价格昂贵，一般不会选择其作为家庭网络的主要传输介质。家庭网络通常会选择双绞线作为主机的传输介质。

双绞线分为屏蔽双绞线与无屏蔽双绞线，两者主要的不同是增加了一层金属屏蔽护套。这层屏蔽护套的主要作用是为了增强其抗干扰性，同时可以在一定程度上改善其带宽。但是由于屏蔽双绞线的价格比无屏蔽双绞线贵，安装也比较困难，加之家庭中网络结构简单，设备少，所以没有必要使用屏蔽双绞线。在 EIA/TIA-568A 标准中，推荐使用的是：4 对 100Ω 五类 UTP（无屏蔽双绞线）。4 对是指一根线套内有 4 个双绞对，共 8 根线，如图 1-6 所示。

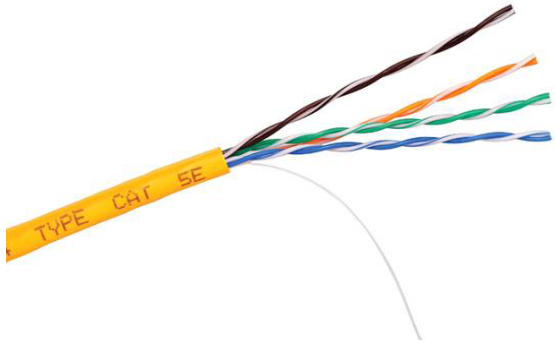


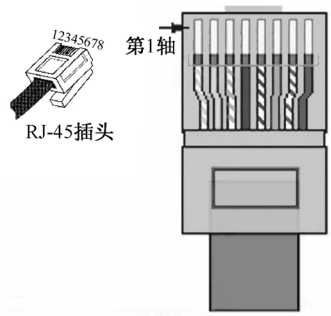
图 1-6　超五类非屏蔽双绞线

（3）双绞线的制作

双绞线的制作主要遵循 EIA/TIA 标准，规范两种双绞线的标准为 EIA/TIA 568A 和 EIA/TIA 568B，这两种标准的线序有所区别，目前主要使用 EIA/TIA 568B 标准。如图 1-7 和图 1-8 所示。

EIA/TIA568A 双绞线的标准制作方法：

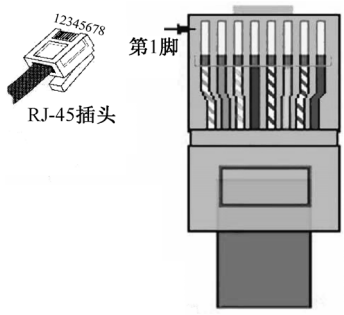
引 脚 顺 序	介质直接连接信号	双绞线绕对的排列顺序
1	TX+（传输）	白绿
2	TX-（传输）	绿
3	RX+（接收）	白橙
4	没有使用	蓝
5	没有使用	白蓝
6	RX-（接收）	橙
7	没有使用	白棕
8	没有使用	棕
EIA/TIA568A 标准见图 1-7		



RJ-45型网线插头的T568A线序

图 1-7　T568A 标准

引 脚 顺 序	介质直接连接信号	双绞线绕对的排列顺序
1	TX+（传输）	白橙
2	TX-（传输）	橙
3	RX+（接收）	白绿
4	没有使用	蓝
5	没有使用	白蓝
6	RX-（接收）	绿
7	没有使用	白棕
8	没有使用	棕
EIA/TIA568B 标准见图 1-8		



RJ-45型网线插头的T568B线序

图 1-8　T568B 标准

EIA/TIA568B　双绞线的标准制作方法：

根据双绞线两端水晶头的制作方法不同，双绞线制作还有直通线和交叉线之分。

- 直通线的标准制作方法

水晶头两端都是遵循 568A 或 568B 标准，双绞线的每组绕线是一一对应的，如图 1-9 所示。直通线通常用于连接导型设备，例如计算机和交换机间的连接。

图 1-9　直通线的制作方法

- 交叉线的标准制作方法

水晶头一端遵循 568A 标准，而另一端遵循 568B 标准。交叉线一般用来连接异型设备，如两个计算机间的连接，如图 1-10 所示。

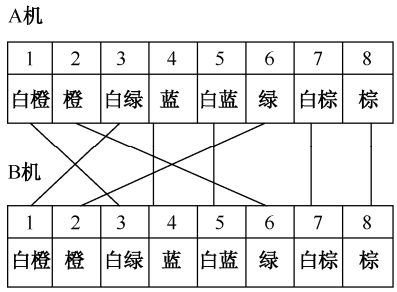


图 1-10　交叉线

（4）集线器

网络集线器，它和双绞线等传输介质一样，是一种不需任何软件支持或只需很少管理软件管理的硬件设备。它被广泛应用到各种场合。集线器工作在局域网（LAN）环境，像网卡一样，应用于OSI 参考模型第一层，因此又被称为物理层设备。集线器实际上就是中继器的一种，其区别仅在于集线器能够提供更多的端口服务，所以集线器又叫多口中继器，如图 1-11 所示。

图 1-11　网络集线器

网络集线器属于纯硬件网络底层设备，基本上不具有类似于交换机的“智能记忆”能力和“学习”能力。它发送数据时都是没有针对性的，而是采用广播方式发送。当它要向某结点发送数据时，不是直接把数据发送到目的节点，而是把数据包发送到与集线器相连的所有节点。

集线器在局域网中只能起到信号放大、传输的作用，不能对信号中的碎片进行处理，所以在传输过程中非常容易出错。从它们的工作状态看，集线器属于共享型。在一个端口向另外一个端口发送信息的时候，其它的端口就不能再有信息传输，只能处于等待状态。另外，集线器是工作在半双工下，即在传输过程中只能是单向的，必须是在一个发送源发送完信息后，接受方才能发送信号。

（5）网络交换机

网络交换机又称“网络交换器”，是一个扩大网络的器材，能为网络中提供更多的连接端口，以便连接更多的计算机。在局域网中一般称为以太网交换机，以太网交换机是基于以太网传输数据的交换机，以太网交换机的结构是每个端口都直接与主机相连，并且一般都工作在全双工方式。交换机能同时连通许多对端口，使每一对相互通信的主机都能像独占通信媒体那样，进行无冲突地传输数据。以太网交换机工作于 OSI 网络参考模型的第二层（即数据链路层），是一种基于 MAC（Media Access Control，介质访问控制）地址识别、完成以太网数据帧转发的网络设备，如图 1-12 所示。

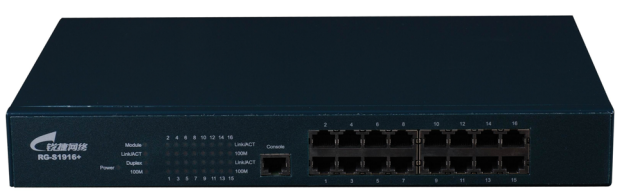


图 1-12　网络交换机

交换机上用于链接计算机或其他设备的插口称作端口。计算机借助网卡通过网线连接到交换机的端口上。网卡、交换机和路由器的每个端口都具有一个 MAC 地址，由设备生产厂商固化在设备的 EPROM 中。MAC 由 IEEE 负责分配，每个 MAC 地址都是全球唯一的。MAC 地址是长度为 48 位的二进制，前 24 位由设备生产厂商标识符，后 24 位位生产厂商自行分配的序列号。

交换机在端口上接受计算机发送过来的数据帧，根据帧头的目的 MAC 地址查找 MAC 地址表然后将该数据帧从对应端口上转发出去，从而实现数据交换。交换机的工作过程可以概括为“学习、记忆、接收、查表、转发”等几个方面：通过“学习”可以了解到每个端口上所连接设备的 MAC 地址；将 MAC 地址与端口编号的对应关系“记忆”在内存中，生产 MAC 地址表；从一个端口“接收”到数据帧后，在 MAC 地址表中“查找”与帧头中目的 MAC 地址相对应的端口编号，然后，将数据帧从查到的端口上“转发”出去。

交换机与集线器对比，交换机可以看作是一种智能型的集线器，它除了包括集线器的所有特性外，还具有自动寻址、交换、处理的功能。并且在传递过程中，只有发送源与接收源独立工作，期间不与其它端口发生关系，从而达到防止数据丢失和提高吞吐量的目的。交换机的工作原理却与集线器有很大区别，由于它的每个端口都可视为一条独立的通道，所以在一个端口工作时不会影响到其它端口的传输。交换机是工作在全双工状态下的，因此它的数据处理能力在无形中又提高了一倍。

（6）路由器

路由器（Router）又称网关设备（Gateway）是用于连接多个逻辑上分开的网络，所谓逻辑网络是代表一个单独的网络或者一个子网。当数据从一个子网传输到另一个子网时，可通过路由器的路由功能来完成。因此，路由器具有判断网络地址和选择 IP 路径的功能，它能在多网络互联环境中，建立灵活的连接，可用完全不同的数据分组和介质访问方法连接各种子网，路由器只接受源站或其他路由器的信息，属网络层的一种互联设备。

路由器按性能档次分为高、中、低档路由器，从结构上分为“模块化路由器”（如图 1-13 所示）和“非模块化路由器”，按所处网络划分通常把路由器划分为“边界路由器”和“中间节点路由器”，从性能上可分为“线速路由器”以及“非线速路由器”，从功能上划分，可将路由器分为“级路由器”，“企业级路由器”和“接入级路由器”等。生活中最常见的家庭路由器就是属于接入级路由器，如图 1-14 所示。

图 1-13　锐捷模块式路由器

图 1-14　家用无线路由器

3）IP 地址

因特网（internet）是国际计算机互联网的英文称谓。因特网以 TCP/IP 网络协议将各种不同类型、不同规模、位于不同地理位置的物理网络联接成一个整体。它把分布在世界各地、各部门的计算机通过网络线路联接起来，从而进行通信和信息交换，实现资源共享。

IP 是英文 Internet Protocol 的缩写，意思是“网络之间互连的协议”，也就是为计算机网络相互连接进行通信而设计的协议。在因特网中，它是能使连接到网上的所有计算机网络实现相互通信的一套规则，规定了计算机在因特网上进行通信时应当遵守的规则。任何厂家生产的计算机系统，只要遵守 IP 协议就可以与因特网互连互通。正是因为有了 IP 协议，因特网才得以迅速发展成为世界上最大的、开放的计算机通信网络。因此，IP 协议也可以叫做“因特网协议”。常见的 IP 地址，分为 IPv4 与 IPv6 两大类。

（1）IPv4 的地址

IP 地址可分为 IPv4 版本和 IPv6 版本，IPv6 是下一版本的互联网协议，IPv4 版本是目前正在使用的互联网协议，由网络 ID+主机 ID 构成，分别代表网络域和主机域。这种二层结构的 IP 地址划分方案称为标准 IP 地址划分方案。其表示格式为 4 个字节的数字串，每个字节用小数点隔开。每个字节可以用二进制、十进制、十六进制表示。每个字节用二进制表示占 8 位，共计 32 位。

（2）IP 地址的分类

目前 IPv4 版本的 IP 地址共分为 5 类：A 类、B 类、C 类、D 类、E 类，各类地址的空间及容量见表 1-1。

表 1-1　IPv4 地址的空间及容量

地 址 类 型	十进制首字节范围	二进制固定最高位	二进制网络位	二进制主机位	网　络　数	主　机　数
A 类	0～127	0	8 位	24 位	$2^{8-1}-2=126$	$2^{24}-2=16777214$
B 类	128～192	10	16 位	16 位	$2^{16-2}=16394$	$2^{16}-2=65534$
C 类	192～223	110	24 位	8 位	$2^{24-3}=2097152$	$2^{8}-2=254$
D 类	224～239	1110	组播地址，用于多点播送			
E 类	240～255	11110	保留给试验使用			

在 A、B、C 三类 IP 地址中包换共计 273 个地址块归内部网络使用，为私网地址，分别是：

- A 类地址中的 1 个私有网络，地址范围是：10.0.0.0~10.255.255.255；
- B 类地址中的 16 个私有网络，地址范围是：172.16.0.0~172.31.255.255；
- C 类地址中的 256 个私有网络，地址范围是：192.168.0.0~192.168.255.255；
- 其它为公网地址。

具有特殊意义的 IP 地址，其形式见表 1-2。

表 1-2　IPv4 特殊意义的 IP 地址

特 殊 地 址	网　络　位	主　机　位	可当作源地址	可当作目的地址
网络地址	网络 ID	全 0	是	是
回送地址	127	任意数	是	是
本网络的本台主机	全 0	全 0	是	否
本网络的某台主机	全 0	主机 ID	否	是
直接广播地址	网络 ID	全 1	否	是
受限广播地址	全 1	全 1	否	是

（3）子网掩码

IP 地址包含网络地址和主机地址两个部分，计算机通过子网掩码来计算，以区分出 IP 地址中的网络部分与主机部分，IPv4 使用默认子网掩码分别是：

A 类是 255.0.0.0

B 类是 255.255.0.0

C 类是 255.255.255.0

家庭局域网通常使用 C 类的私有 IP 地址段，如 C 类网络 192.168.1.0/24，该网络中可用的 IP 地址是 192.168.1.1 至 192.168.1.254，子网掩码是 255.255.255.0。

2．宽带接入网

1）宽带接入网方式

随着网络的普及，越来越多的家庭也需要连接互联网，在我国家庭网络宽带接入方式主要有以下 4 种：

（1）ADSL

ADSL 是目前 xDSL 中最常用的一种技术。它是非对称数字用户环路技术的英文简称，它充分利用了现有固定电话网的电缆资源，可以在不影响正常电话通信的情况下，通过一条电话线，同时实现电话通信、数据业务互不干扰的传送方式。其业务特点如下：

- 上行速率最高达 640kbps，下行速率最高达 8Mbps。
- 速率不对称：上下行速率不相等。
- 节省费用：上网独立于打电话，可以与电话同时使用，互不影响。
- 安装简易：只需在普通电话线上加语音分离器和 ADSL Modem，计算机中加上网卡即可使用，安装十分简单。

ADSL 通过二线（电话线）连接局端设备与用户端“猫”，线上传输高频信号。由于其技术特性，有以下几个限制：

- 传输距离为 2.5km 左右；
- 速率受距离、线径、干扰等环境影响较大。

因此，为保证用户正常使用，一般速率控制在 2Mbps 以内。

（2）VDSL

VDSL 是甚高速数字用户环路技术的英文简称，简单来说，VDSL 技术就是 ADSL 的快速版本。采用 VDSL 技术，在较短距离内可以获得比 ADSL 技术更高的传输速率，VDSL 的最大下行速率可达 55Mbps，上传速率可达 19.2Mbps。VDSL 传输距离为 500～1000m 左右，速率受距离、线径、干扰等环境影响较大。因此，为保证用户正常使用，目前提供 10Mbps 上、下行对称速率。

（3）LAN

以太网宽带接入（FTTx+LAN）是一种光纤加五类网络线的宽带接入方式。它将光纤直接接入小区和大楼，然后通过五类线与各用户的终端相连，为广大用户提供高速上网和其他宽带数据服务。LAN 具有传输速率高、用户端投资少的特点。可以满足不同层面用户的多种需求。

业务特点：

- 传输速率高，网络稳定性好。
- 安装方便，用户端投资省。

注意：电信的 LAN 与其它运营商的 LAN 有很大的区别。电信 LAN 是采用 VLAN 方式，个人独享 VLAN 及带宽，屏蔽操作系统的各类广播包，具有速度快，保密性好的特点。

（4）光纤专线接入

光纤接入是指局端与用户之间完全以光纤作为传输媒体。光纤接入可以分为有源光接入和无源光接入。光纤用户网的主要技术是光波传输技术。目前光纤传输的复用技术发展相当快，多数已处于实用化。

目前我国家庭使用最多的网络宽带接入方式还是 ADSL 宽带接入技术。ADSL 宽带接入技术主要采用 PPPOE 虚拟拨号连接互联网的技术，由于微软的操作系统中自带拨号连接程序，所以 PPPOE 虚拟拨号连接因特网也成为现代人们分享资源，进行信息交流的主要方式。如图 1-15 所示。

图 1-15　Windows XP 系统的 PPPoE 拨号程序

2）基于 ADSL 的家庭网络

用户端 ADSL 设施包括数据/语音分离器、ADSL Modem、电话机、计算机等设备。分离器的作用是把语音信号分离出来供电话使用，并阻止电话对宽带信号的干扰。多数分离器一侧有一个标记为“LINE”的端口，用于连接入户的电话线；另一侧有两个端口，标记为“PHONE”的端口用于连接电话机，标记为“DSL”的端口用于连接 ADSL Modem。如果将电话机连接到 DSL 端口或分离器的前端，都将影响上网质量，甚至无法上网。家庭单机环境连接 Internet 如图 1-16 所示。

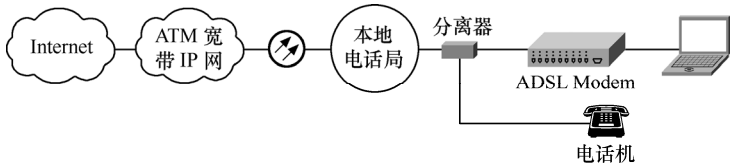


图 1-16　基于 ADSL 的家庭网络单机环境

如果是多台计算机的环境下，则需要一个带有路由功能的 ADSL Modem，这种具有路由功能的 ADSL Modem 可当作一台主机来用，由 Modem 提供 NAT（将内网 IP 地址转换为公网 IP 地址）功能。将 ADSL Modem 的“DSL”端口直接连在集线器上，集线器连接办公计算机。ADSL Modem 的其他接口连接同家庭网络，如图 1-17 所示。

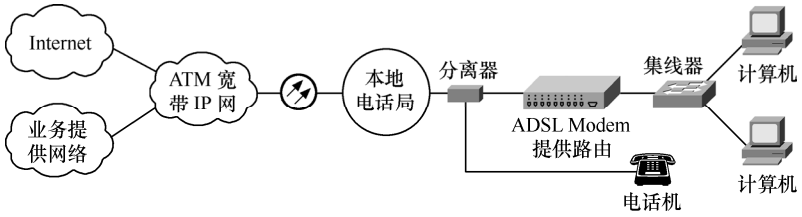


图 1-17　基于 ADSL 的家庭网络多机环境

3．家庭无线局域网

无线局域网（WLAN）产业是当前整个数据通信领域发展最快的产业之一。因其具有灵活性、可移动性及较低的投资成本等优势，无线局域网解决方案作为传统有线局域网络的补充和扩展，获得了家庭网络用户、中小型办公室用户、广大企业用户及电信运营商的青睐，得到了快速的应用。随着掌上移动设备的增多，例如像智能手机、IPAD 等这样的产品，也可以通过家庭无线网络方便地接入因特网，实现随时随地上网。

图 1-18　无线路由器背面端口

1）无线路由器

家用无线路由器就是家用计算机上网用的一种分配器，家庭中有超过两台的计算机，就可以通过无线路由器使用一根电话线同时上网而不相互影响，让家庭内多台计算机共享一个账号上网，如图 1-18 所示。

2）认识端口

（1）外网接口（WAN）：用于连接外网，如宽带接入，或和用于拨号的猫（Modem）连接。

（2）内网接口（LAN）：用于和台式机或其他支持 RJ-45（普通网线）接口的设备连接。

（3）复位：用于恢复路由出厂设置，在接通电源时，按下复位按钮几秒钟等指示灯全亮时松开，即可将路由恢复到出厂设置。

3）常用的无线协议

与有线局域网不同，无线局域网常用的协议主要包括 802．11b、802．11a、802．11g 与 802.11n 协议。各协议的使用频段与传输速率如表 1-3 所示。

表 1-3　常用无线协议的频段和传输速率

协　议	频　段	传 输 速 率
802.11b	2.4GHz	11Mbps
802.11a	5GHz	54Mbps
802.11g	2.4GHz	54Mbps
802.11n	2.4GHz 和 5GHz	108Mbps 最高可达 302Mbps

4）无线加密方式

家庭无线路由器中，无线网络加密方式一般有三种：WEP、WPA 以及 WPA-PSK，如图 1-19 所示。

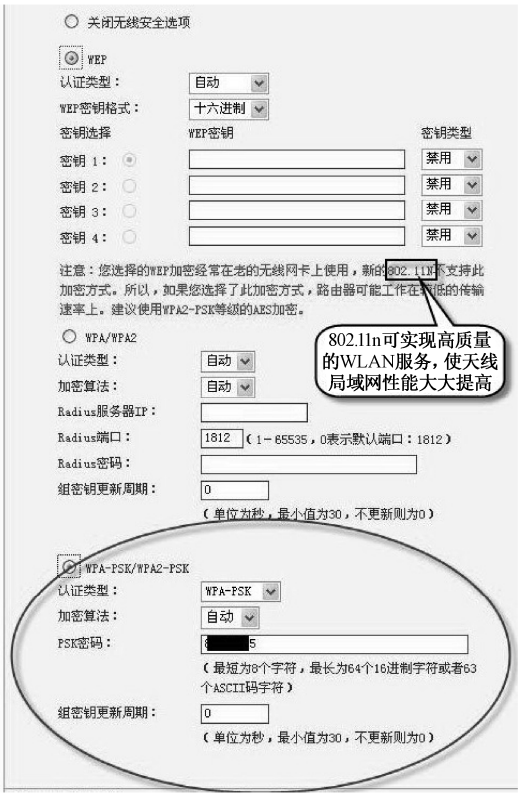


图 1-19　常见的无线加密方式

（1）WEP 安全加密方式

WEP 的全称是：802.11 Wired Equivalent Privacy，它是无线网络第一个安全协议，WEP 特性里使用了一种称为 rc4 prng 的算法。所有客户端和无线接入点都会以一个共享的密钥进行加密，密钥越长，就越安全。WEP 的缺点是：使用的是静态的密钥非动态密钥，很容易被黑客破解。

（2）WPA 安全加密方式

WPA 的全称是：Wi-Fi Protected Access，作为 WEP 的升级版，在安全性上有了很大的改进，主要体现在身份认证、加密机制和数据包检查等方面。WPA 的优点是：使用了动态的密钥。

缺点是：完整的 WPA 设置是比较复杂的，由于操作过程比较困难，一般用户很难设置。

（3）WPA-PSK 安全加密方式

由于 WPA 操作复杂，因此在家庭网络中经常采用的是 WPA 的简化版：WPA－PSK。WPA-PSK 可以看成是一个认证机制，只要求一个单一的密码进入每个无线局域网节点（例如无线路由器），只要密码正确，就可以使用无线网络。加密机制和 WPA 是相同的。两者的区别是：WPA-PSK 认证被简化为只要一个简单的密码，而不需要设置复杂的身份证明等信息。WPA-PSK 的缺点是：同 WEP 一样也会受到黑客的破解。但是因为密钥是动态的，其安全性比 WEP 要强很多。

考虑到家庭网络比较简单，最好选择 WPA-PSK 的加密方式，同时注意定期更换密码，但是如果家中有一些比较老的设备只能支持 WEP 的方式，那就只有尽量加大密码的长度或者更换设备来解决了。

项目实施

任务一　实现 ADSL 宽带上网

任务描述

张先生一家有四口人，家里原来只有一台计算机，最近因为儿子、女儿的学习需要，张先生为他们各添加了一台计算机。现在需要把家里的 3 台计算机连接起来，组建家庭网络环境，实现文件共享，并且实现所有计算机都可以连接因特网。

网络拓扑

家庭网络拓扑结构如图 1-20 所示。

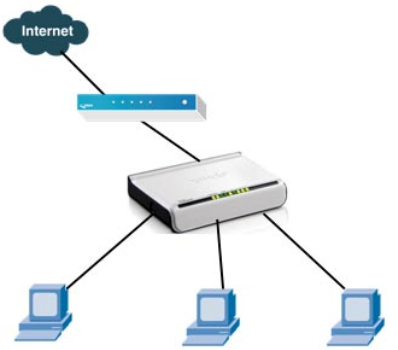


图 1-20　家庭网络拓扑结构图

任务目标

制作 3 条双绞线，连接到 3 台计算机，实现 3 台计算机互通；调试家庭无线路由器，实现共享上网。

设备清单

家庭路由器 1 台、ADSL Modem 1 台、分离器 1 个、双绞线与水晶头 N 个。

工作过程

步骤一：制作双绞线

制作 RJ-45 网线插头是组建局域网的基础技能，制作方法并不复杂。实质就是把双绞线的 4 对 8 芯网线按一定的规则制作到 RJ-45 插头中。制作最常用的遵循 T568B 标准的直通线为例，制作过程如下：

第 1 步：用双绞线网线钳把双绞线的一端剪齐然后把剪齐的一端插入到网线钳用于剥线的缺口中。顶住网线钳后面的挡位以后，稍微握紧网线钳慢慢旋转一圈，让刀口划开双绞线的保护胶皮并剥除外皮，如图 1-21 所示。

注意：网线钳挡位离剥线刀口长度通常恰好为水晶头长度，这样可以有效避免剥线过长或过短。如果剥线过长往往会因为网线不能被水晶头卡住而容易松动，如果剥线过短则会造

成水晶头插针不能与双绞线完好接触。

第 2 步：剥除外包皮后会看到双绞线的 4 对芯线，每对芯线的颜色各不相同。将绞在一起的芯线分开，按照橙白、橙、绿白、蓝、蓝白、绿、棕白、棕的颜色一字排列，并用网线钳将线的顶端剪齐，如图 1-22 所示。

图 1-21　网线钳剥线

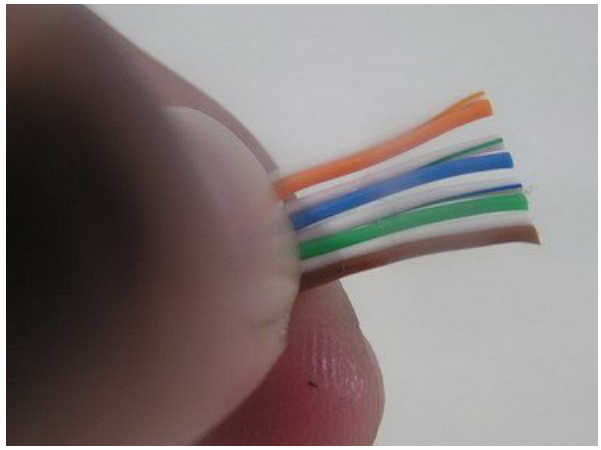


图 1-22　按 T568B 线序排列

第 3 步：使 RJ-45 插头的弹簧卡朝下，然后将正确排列的双绞线插入 RJ-45 插头中。在插的时候一定要将各条芯线都插到底部。由于 RJ-45 插头是透明的，因此可以观察到每条芯线插入的位置，如图 1-23 所示。

第 4 步：将插入双绞线的 RJ-45 插头插入网线钳的压线插槽中，用力压下网线钳的手柄，使 RJ-45 插头的针脚都能接触到双绞线的芯线，如图 1-24 所示。

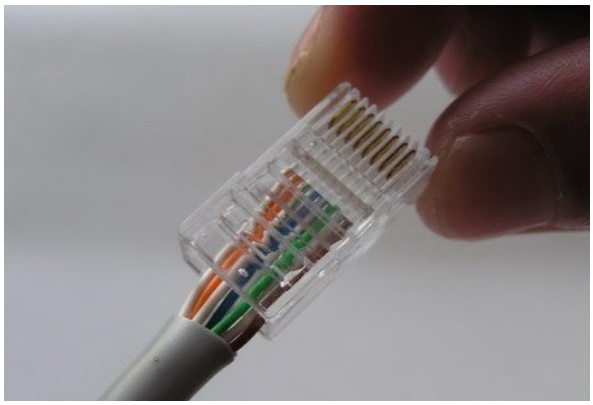


图 1-23　将双绞线插入水晶头

图 1-24　用压线钳压紧

第 5 步，完成双绞线一端的制作工作后，按照相同的方法制作另一端即可。注意双绞线两端的芯线排列顺序要完全一致。

第 6 步：在完成双绞线的制作后，建议使用网线测试仪对网线进行测试。将双绞线的两端分别插入网线测试仪的 RJ-45 接口，并接通测试仪电源。如果测试仪上的 8 个绿色指示灯都顺利闪过，说明制作成功。如果其中某个指示灯未闪烁，则说明插头中存在断路或者接触不良的现象。如图 1-25 所示。

步骤二：按照拓扑图，连接设备

连接方式如图 1-26 所示。

图 1-25　双绞线测试

图 1-26　具体连接图

第 1 步：电话进线连接到 ADSL 语音分离器的 LINE 接口。

第 2 步：分离器的 Phone 接口连接到电话机。

第 3 步：分离器的 Moden 接口连接到 ADSL Modem 的 ADSL 接口。

第 4 步：ADSL Modem 的 LAN 接口用网线连接到路由器的 WAN 接口。

第 5 步：路由器的 LAN 接口连接到计算机的网卡。

步骤三：进行路由器设置

第 1 步：查看路由器背面的管理 IP 地址，并设置计算机的 IP 地址与路由器管理 IP 在同一个段。

图 1-27　路由器管理 IP

设置 IP 地址步骤：使用鼠标右键单击“网上邻居”，选择属性 →“本地连接”→“属性”→“TCP/IP”→“属性”→设置，如图 1-28 所示的 IP 地址。

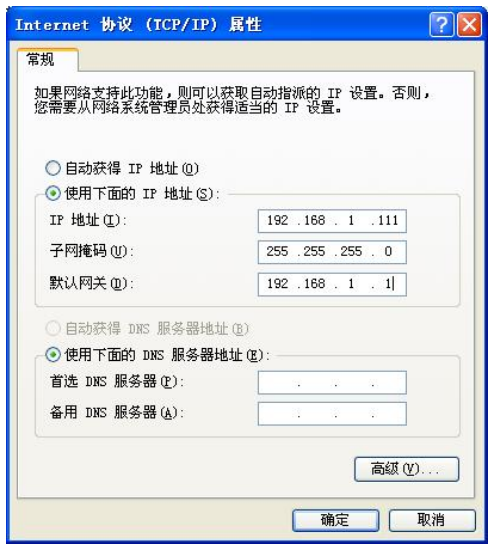


图 1-28　设置 IP 地址

设置完成后，可通过在“开始”→“运行”中输入“ping 192.168.1.1”命令来测试计算机与路由器管理 IP 的连通性，如图 1-29 所示。

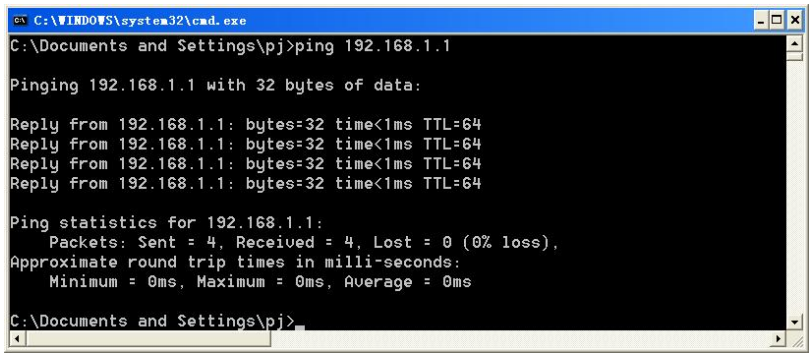


图 1-29　设置 IP 地址

第 2 步：打开 IE 浏览器，在地址栏输入“192.168.1.1”，进行相关的设置。

第 3 步：在设置页面中单击“设置向导”→“下一步”按钮

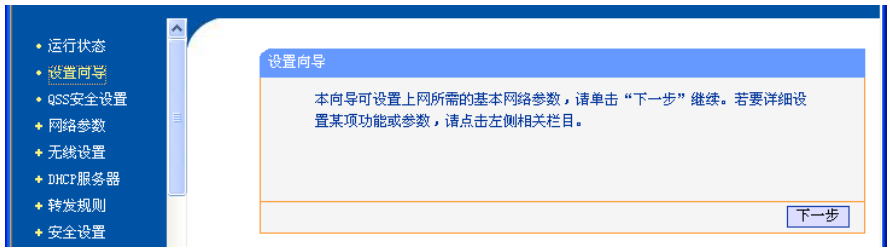


图 1-30　单击“设置向导”

第 4 步：在如图 1-31 所示的页面中选择“PPPoE（ADSL 虚拟拨号）”。

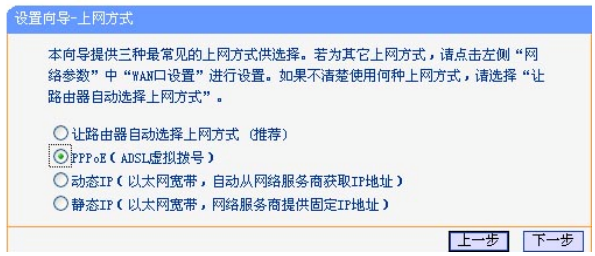


图 1-31　选择 PPPoE

第 5 步：以图 1-32 中输入 ADSL 拨号的上网账号和上网口令。

图 1-32　输入上网的账号和口令

第 6 步：在图 1-33 中，单击“重启”按钮后，即可以实现上网了。

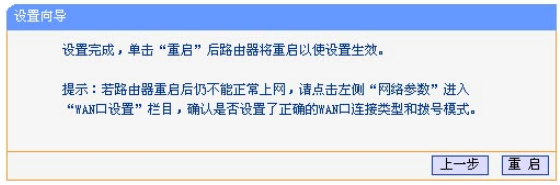


图 1-33　设置完成

第 7 步：为了免除设置 IP 地址的麻烦，一般需要设置 IP 自动分配，依次单击“DHCP 服务器”→“DHCP 服务”，具体设置如图 1-34 所示。

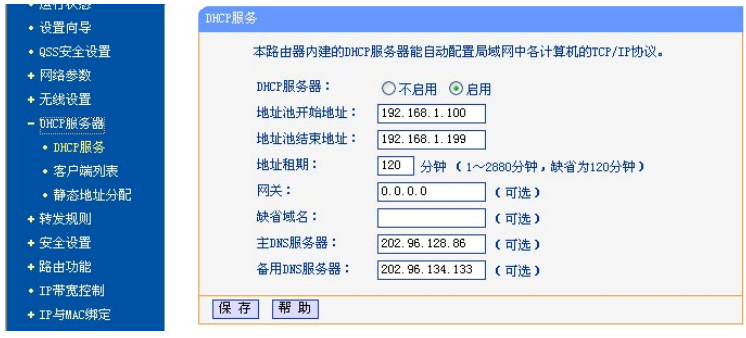


图 1-34　设置 DHCP 服务器

第 8 步：单击“保存”按钮，重启路由器后，设置真正完成。

项目测试

第 1 步：设置自动获取 IP 地址，依次点击“本地连接”→“属性”→“TCP/IP”→“属性”→“自动获得 IP 地址”和“自动获得 DNS 服务器地址”，如图 1-35 所示。

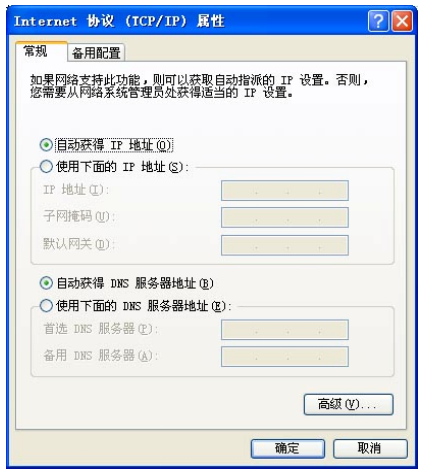


图 1-35　自动获取 IP 地址

第 2 步：可使用“ipconfig”命令查看获取到的 IP 地址，如图 1-36 所示。

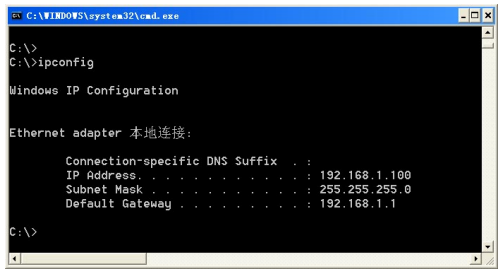


图 1-36　ipconfig 查看命令

第 3 步：可使用 ping 命令测试到路由器的连通性，也可以打开网页测试是否正常。如图 1-37 所示。

图 1-37　打开网页测试

任务二　实现移动设备无线上网

任务描述

张先生新购买了一台智能手机，并且准备为孩子购买 iPad，希望在家里设置一个无线网络，

让手机和 iPad 等移动设备能够通过家庭的无线网络连接到因特网。

网络拓扑

网络拓扑如图 1-38 所示。

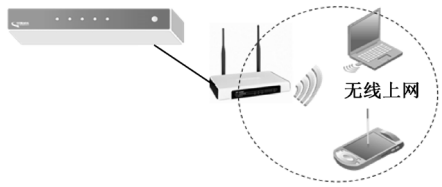


图 1-38　设置无线路由器实现无线上网

任务目标

设置需购买一个家庭无线路由器，开启无线功能，开启无线密码防止非法用户接入，设置笔记本和智能手机连接家庭无线网络，实现上网。

设备清单

家庭无线路由器 1 台、ADSL Modem 1 台、分离器 1 个、双绞线与水晶头 N 个。

工作过程

步骤一：将原路由器更换为家庭无线路由器，并正确的连接线缆。

步骤二：打开 IE 浏览器，在地址栏输入“192.168.1.1”，进行无线的相关设置。

第 1 步：在页面中依次单击“无线设置”→“基本设置”，如图 1-39 所示，进行相关设置。

图 1-39　无线网络基本设置

第 2 步：在页面中依次单击“无线设置”→“无线安全设置”，如图 1-40 所示，进行相关设置。

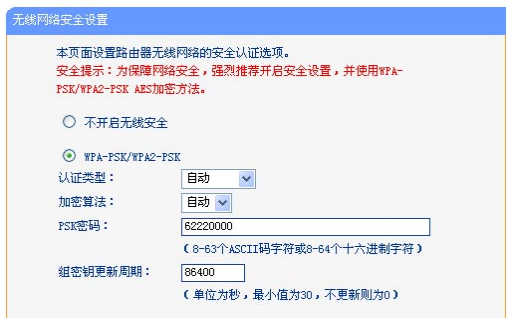


图 1-40　无线网络安全设置

第 3 步：为使设置生效，需要重新启动路由器。在页面中依次单击“系统工具”→“重启路由器”，如图 1-41 所示。

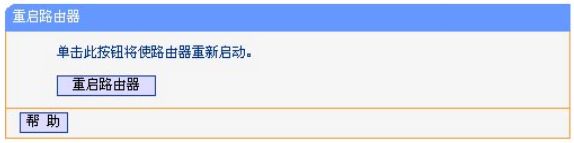


图 1-41　重启路由器

项目测试

第 1 步：打开笔记本电脑，依次单击“网上邻居”→“属性”→“无线网络连接”→“查看可用的无线连接”如图 1-42 所示。

第 2 步：“选择 SSID 为 McDull 的无线信号”→“连接”→“输入网络密钥”→“连接”，查看验证密码成功后，显示已连接无线网络，如图 1-43～图 1-45 所示。

图 1-42　查看可用的无线连接

图 1-43　选择无线网络

图 1-44　输入无线网络密钥

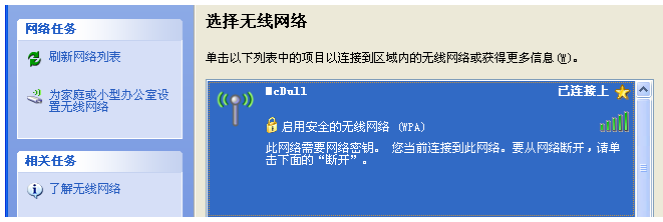


图 1-45　已连接上 McDull

第 3 步：打开网页测试，如图 1-46 所示。

图 1-46　测试网络

认证测试

一、选择题

1．通常使用以下哪条命令测试到路由器的连通性（　　）。

A．ping　　B．ipconfig　　C．netstat　　D．nbtstat

2．常见的无线加密方式不包括（　　）。

A．WEP　　B．WPA　　C．WPA-PSK　　D．DES

3．下列哪条命令是显示计算机网络参数的命令（　　）。

A．ipconfig　　B．show interface Ethernet 0/0/1

C．ipconfig/all　　D．show running-config

4．交换机是通过以下（　　）来进行数据交换的。

A．IP　　B．MAC　　C．标识　　D．接口

5．家庭网络拓扑结构通常使用（　　）拓扑。

A．总线型　　B．星形　　C．树形　　D．网状形

二、简答题

1．MAC 地址是如何构成的？MAC 地址的作用是什么？

2．描述广播域、冲突域的定义。

3．说明集线器与交换机的区别。

项目二　商畅数码有限公司网络配置与管理

项目背景

商畅数码有限公司是一家新成立的小型企业，位于广州天河区，主要从事数码产品的研发与销售业务，现已经在五山大厦租下了一层楼作为公司的办公场地。公司有行政部、研发部、财务部和销售部 4 个部门共计 21 名员工，每一个员工都有一台计算机用于办公。目前新成立的公司还没有建好网络，各部门间的文件、资料、打印机共享不了，这些问题影响了公司业务的正常进行，公司王总决定马上进行公司网络的组建，并委托网络管理员小李进行公司网络的设计与具体的施工，为了公司的数据安全，要求部门间的网络要隔离，所有计算机都能够相互通信。

公司办公环境如图 2-17 所示。

图 2-1　公司办公环境

项目分析

分析一：需要将所有办公室的计算机通过网线连接到交换机上，并通过交换的配置，实现不同部门的网络隔离。

分析二：需要使用路由器实现所有计算机都能够相互通信。

项目方案

商畅数码有限公司属于小型企业，网络结构简单，可采用星形拓扑结构。目前公司有 4 个部门 21 台计算机，可选用 1 台 24 口的交换机，实现所有计算机的连接；通过在交换机上进行 VLAN 配置，实现部门间网络的隔离；通过配置路由器，实现不同部门的计算机相互通信。其网络拓扑结构如图 2-2 所示。

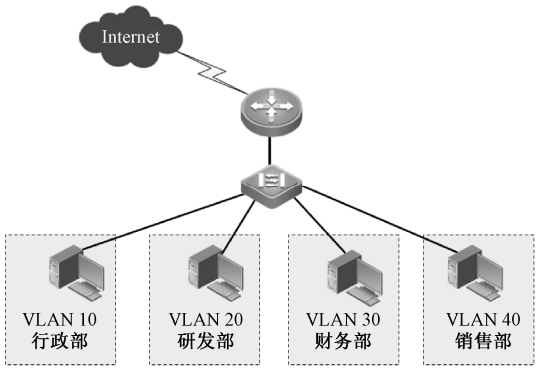


图 2-2　网络拓扑图

知识准备

1．交换机配置基础

1）交换机外形结构

不同产家，不同型号的设备外形结构也不同，具体可参考产家的产品说明书。如锐捷 S2126G 交换机和神州数码的 DCS3950 交换机的前面板如图 2-3 和图 2-4 所示。

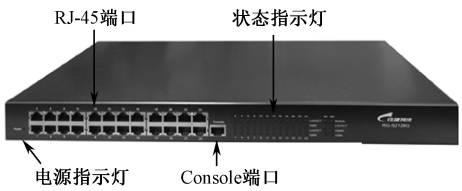


图 2-3　锐捷交换机前面板

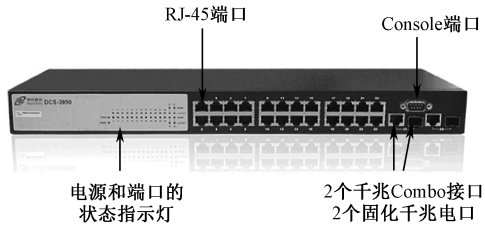


图 2-4　神州数码交换机前面板

（1）交换机端口识别

- 24 个 10Base-T/100Base-TX RJ-45 端口：接 5 类 UTP 或 STP 的双绞线。
- 2 个千兆模块端口（Combo 接口）：可接 1000Base-SX 的多模光纤模块；1000Base-LX 的单模光纤模块。例如，图 2-4 中神州数码交换机的 2 个千兆 Combo 接口和 2 个固化千兆电口是光电复用接口，同样都是 25 号端口，可接光纤和千兆网络，但同时只能用其中一个。
- Console 串口：连接配置的反转线，如图 2-5 所示。

（2）RJ-45 端口状态指示灯的具体含义如下

- Link/ACT：绿灯闪状态，表示正在传递数据；绿灯亮状态，表示链路连通；灯灭状态，表示链路不通；
- 100Mb/s LED：灯亮状态，表示速率为 100Mbps

（3）千兆模块端口状态指示灯的具体含义如下。

- Link/ACT：同 RJ-45 端口 Link/ACT 描述；
- 1000Mb/s：灯亮表示速率为 1000Mbps；
- 100Mb/s：灯亮表示速率为 100Mbps。

2）交换机分类

交换机是局域网中重要的组网设备，可以通过配置交换机，使网络具有可管理功能，优化网络的性能。按是否具有管理功能，交换机可分为可管理交换机和不可管理交换机。不可管理的交换机如集线器一样，接上网线后可直接使用，不具有智能化；而可网管交换机具有管理、控制网络等智能化管理功能，如端口监控、划分 VLAN、配置环路避免等特性。

识别两种交换机的方法是看是否有配置口，可网管交换机一般有 Console 端口，如图 2-5 所示，并配有 Console 线，如图 2-6 所示，而不可网管交换机没有此端口，这成为从外观区分两者的重要标志。

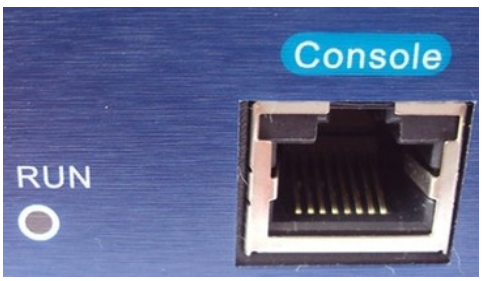


图 2-5　交换机 Console 端口

图 2-6　交换机 Console 线

3）交换机配置方法

（1）交换机管理方式

主要有两种：带外管理与带内管理。带外管理是指网络的管理控制信息与用户网络的承载业务信息在不同的逻辑信道传送，也就是设备提供专门用于管理的带宽；用 Console 线管理就是带外管理的主要方式之一，如图 2-7 所示。

带内管理是指网络的管理控制信息与用户网络的承载业务信息通过同一个逻辑信道传送，简而言之，就是占用业务带宽。带内管理的方式有 Telnet 方式、Web 方式、网管软件方式三种，如图 2-8 所示。

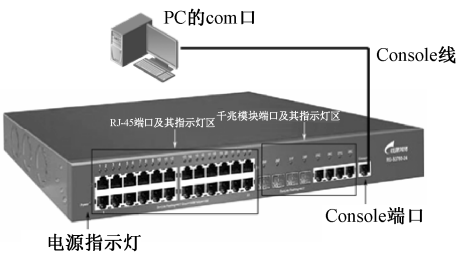


图 2-7　用 Console 登录管理

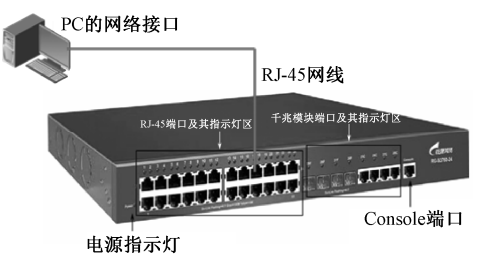


图 2-8　带内管理方式

（2）交换机带外管理配置

交换机带外管理的操作步骤如下：

步骤一：准备好交换机的 Console 线，连接电脑的串口，另一头连接交换机 Console 口进行配置；

步骤二：单击“开始菜单”→“附件”→“通讯”→“超级终端”；

步骤三：建立超级终端连接。在图 2-9 所示界面中，输入新建连接的名称，系统会为用户把这个连接保存在附件中的通信栏中，以便于用户下次使用。单击“确定”按扭。

步骤四：最后一行的“连接时使用”的缺省设置是连接在“COM1”口上，如图 2-10 所示；单

击其下拉菜单，有其他的选项，视用户实际连接的端口而定。

图 2-9　新建连接

图 2-10　使用 com1 口

步骤五：单击右下方的“还原为默认值”按扭，每秒位数为“9600”，数据位为“8”，奇偶校验“无”，停止位为“1”，数据流控制为“无”，如图 2-11 所示，单击“确定”按钮后进入配置模式，如图 2-12 所示。

图 2-11　COM1 口属性设置

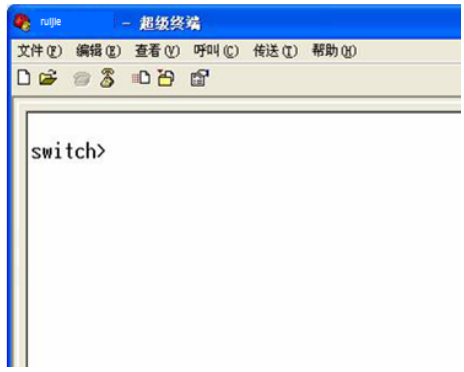


图 2-12　配置模式

4）交换机配置模式

交换机出现如图 2-10 的界面后，表示仿真终端和交换机连接成功，可以进行相应的配置了。交换机首先进入的是用户模式，除此之外交换机的工作模式还有特权模式、全局配置模式、接口配置模式、VLAN 配置模式等方式用来给用户对交换机进行全面的配置和管理。

（1）用户模式的提示符如下：

```
Switch>
```

其中 Switch 是主机名，在该模式下直接输入“？”号并回车可获得该模式下可允许执行的命令清单及说明如：Switch>?

（2）特权模式的提示符如下：

```
Switch#
```

在用户模式下输入 enable 后将进入到特权模式。在该模式下可以对交换机的配置文件进行管理，查看交换机的配置信息，进行网络测试与调试等。返回用户模式可输入“exit”或“disable”命令，重新启动交换机可输入“reload”命令。

（3）全局配置模式的提示符如下：

```
Switch(config)#
```

在特权模式下输入“configure terminal”命令，即可进入到全局配置模式。该模式下可以配置交换机的全局性参数如（如主机名、登录信息等）。返回特权模式，执行“exit”、“end”命令或按【Ctrl+Z】组合键。

（4）接口配置模式的提示符如下：

```
aSwitch(config-if)#
```

在全局配置模式下输入“interface”命令，即进入配置模式。在该模式下，可对选定的接口进行配置，并且只能执行配置交换机端口的命令。

从接口配置模式退回全局配置模式，执行“exit”命令。如退回特权模式，则执行“end”或按【Ctrl+Z】组合键。

（5）VLAN 配置模式的提示符如下：

```
Switch(config-vlan)#
```

在全局配置模式，使用命令“vlan <vlan-id>”命令就可以进入到相应的 VLAN 配置模式。在 VLAN 配置模式，用户可以配置属于本 VLAN 的成员端口。执行“exit”命令即可从 VLAN 配置模式退回到全局配置模式。

5）配置技巧

（1）使用“？”获得帮助

用户在当前命令提示下，输入（?）列出该命令模式可以使用的命令列表。通过不同的方式，使用（?）帮助获得不同帮助效果，如下所示。

```
Switch#?  //查找当前命令
Switch#i? //查找以 i 开始的命令单词
Switch#show ?  //查找 show 命令后面的参数有哪些
```

（2）使用 Tab 键自动补齐命令

```
Switch#con(Tab 键)
Switch#configure terminal
```

（3）使用命令简写

```
Switch>ena（按 Enter 键）
Switch#
```

（4）使用历史命令

交换机系统内存历史缓冲区中记录当前最近使用过的命令，可以使用“↑”和“↓”方向键翻出来重新使用。在“Switch#”按“↑”方向键并回车可使用上一条命令。

6）交换机配置的基本命令

交换机基本配置包括命名交换机、配置管理 IP 地址、设置远程登录密码及特权密码等。

（1）配置设备名称

命令：Switch（config）#hostname *name*

说明：其中：*name* 为新的交换机的主机名，使用该命令的 no 选项将该设置恢复为默认

值，在网络中交换机设备数量比较多的情况下，有利于管理员对网络维护和管理。

案例：将交换机系统名称修改为 abcd。

```
Switch(config)# hostname abcd
abcd(config)#
```

（2）配置管理 IP 地址

交换机管理 IP 地址用于通过 Telnet 方式登录交换机时使用。设置管理 IP 地址后，就可以通过管理 IP 地址登录交换机。

命令：Switch（config-if)# ip address *ip-address mask*

说明：其中：*ip-address* 为端口的 IP 地址；mask 为端口的 IP 掩码。使用该命令的 no 选项将删除指定的 IP 地址。如：Switch（config-if）#no ip address

案例：配置交换机管理 IP 地址为 192.168.1.1。

```
Switch(config)#interface vlan 1   //进入交换机虚拟端口 1
Switch(config-if)#ip address 192.168.1.1 255.255.255.0    //配置虚拟端口 1 的 IP 地址为 192.168.1.1
Switch(config-if)# no shutdown   //激活端口
Switch(config-if)#exit
Switch(config)#show interface vlan 1   //显示 Vlan 1 端口状态
```

（3）配置设备特权模式密码

交换机密码分为特权密码和远程登录密码，其中：特权密码是指从用户模式（Switch>）到特权模式（Switch#）时使用的密码。

命令：Switch（config)#enable secret *[*level *level] {encryption-type encrypted-password}*

说明：level *level* 为口令应用到的交换机的管理级别，可以设置 0 到 15 共 16 个级别，如果不指明级别则默认为 15 级。level15 为特权密码设置。

encryption-type 为加密类型：0 表示用明文输入口令，5 表示用密文输入口令。*encrypted-password* 为输入的口令。如果加密类型为 0，则口令是以明文形式输入；如果加密类型为 5，则口令是以密文形式输入。使用该命令的 no 选项将禁止该级别。如：no enable secret [level *level*]

案例：设置交换机特权密码为 123456，明文方式。

```
Switch#config ter
Switch(config)# enable secret level 15 0 123456
```

（4）交换机配置远程登录密码。

远程登录密码是指通过 Telnet 方式远程登录时使用的密码。交换机远程登录密码命令说明如表 2-1 所示。

表 2-1 交换机远程登录密码命令说明

命 令 格 式	说 明
Switch(config)#line vty *first-line last-line*	其中：*first-line* 为开始线路编号，*last-line* 为结束线路编号
Switch(config-line)#password *password-value*	其中：*password-value* 为登录密码
Switch (config-line)#login	

说明：配置远程登录密码有利于网络设备的安全。

案例：配置远程登录密码为 123456

```
    Switch#config  //进入全局配置模式
    Switch (config)#line VTY 0 4   //0 表示线路 line0,4 表示线路 line4。表示允许 line0 到
line4 共 5 个客户同时登录
    Switch (config-line)#password 123456   //设置登录密码为 123456
    Switch (config-line)#login
```

（5）其他常用命令如表 2-2 所示

表 2-2　其他常用命令

范　例	说　明
Switch# show version	显示系统、版本信息
Switch# show running-config	显示交换机 RAM 里当前生效的配置
Switch# show configure	显示保存在 Flash 里的配置信息
Switch# show interface FastEthernet0/0	显示交换机接口 FastEthernet0/0 信息
Switch# copy running-config startup-config	将保存配置到保存到 Flash 中
Switch(config)# del config.text	删除当前的配置恢复默认值（交换机重启后生效）
Switch# reload	交换将重新启动

2．交换机配置基础

1）什么是虚拟局域网

VLAN（Virtual Area Network）中文意思是虚拟局域网，VLAN 是指在交换局域网的基础上，采用软件处理构建的可跨越不同网段、不同网络的端到端的逻辑网络。一个 VLAN 组成一个逻辑子网，即一个逻辑广播域；它可以是一个交换机的部分端口，也可以是覆盖多个网络设备，允许处于不同地理位置的网络用户加入到一个逻辑子网。如图 2-13 所示，由交换机组成的校园网里面，所有主机都在一个广播域内，VLAN 技术将校园网络划分成了多个广播域，对网络进行了安全隔离。

（1）VLAN 的划分方法

VLAN 的划分方法有很多，如基于端口的划分、基于协议的划分、基于 MAC 地址的划分等。目前主流应用的是基于端口划分，因为基于端口划分简单易用，如图 2-14 所示。

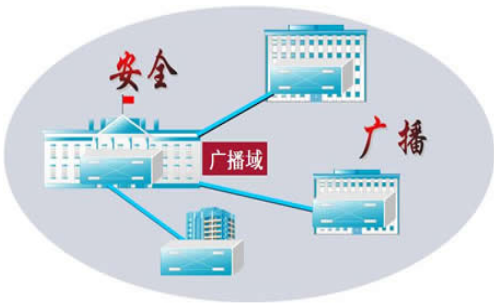


图 2-13　由交换机组成的校园网

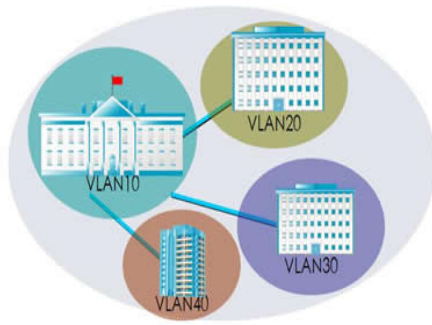


图 2-14　VLAN 的划分

（2）VLAN 的优点

VLAN 建立在局域网交换机的基础上，既保持了局域网的低延迟、高吞吐量特点，又解决了由于单个广播域内广播包过多，网络性能降低的问题。VLAN 技术是局域网组网时经常

使用的主要技术之一，可以有效控制广播域、提高网络安全性、简化网络管理，同时也使得网络的建设和扩展变得方便。VLAN 和一个物理网络一样，每个 VLAN 需要一个 IP 子网 IP 地址。在同一个 VLAN 内的主机应属于同一个 IP 子网。

2．IEEE 802.1q 协议

IEEE 802.1q 协议也就是“Virtual Bridged Local Area Networks”（虚拟桥接局域网，简称“虚拟局域网”）协议，主要规定了 VLAN 的实现方法。IEEE 802.1q 协议为标识带有 VLAN 成员信息的以太帧建立了一种标准方法。IEEE 802.1q 标准定义了 VLAN 网桥操作，从而允许在桥接局域网结构中实现定义、运行以及管理 VLAN 拓扑结构等操作。

IEEE 802.1q 规定了依据以太网交换机的端口来划分 VLAN 的国际标准，同一个 VLAN 中的所有成员共同拥有一个 VLAN ID，组成一个虚拟局域网络；同一个 VLAN 中的成员均能收到同一个 VLAN 中的其他成员发来的广播包，但收不到其他 VLAN 中成员发来的广播包；不同 VLAN 成员之间不可直接通信，需要通过路由器支持才能通信，而同一 VLAN 中的成员通过 VLAN 交换机可以直接通信，不需路由支持。

VLAN 的概念是基于以太网交换的，传统以太网交换原理可以概括为“根据源 MAC 进行学习，根据目的 MAC 进行转发”图 2-15 是传统以太网数据帧：

与标准的以太网帧相比，802.1q 协议加入了 Tag 字段，加入 Tag 的目的是为了携带 VLAN 的信息，这表明了这个数据帧属于哪个 VLAN，以确定数据帧的属性，图 2-16 是一个 802.1q 标准帧格式。

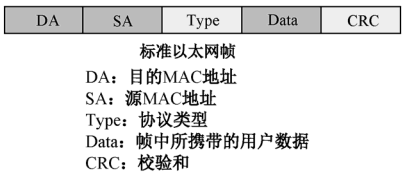


图 2-15　传统以太网数据帧

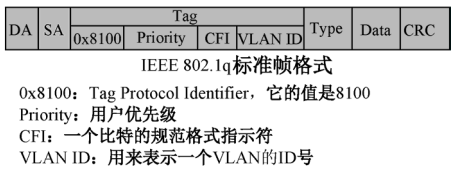


图 2-16　802.1q 标准帧格式

802.1q 协议，可以将网络划分成多个子网，每个子网对应一个 VLAN。当数据帧流经交换机时，交换机会按照 802.1q 标准定义的帧格式对其重新进行封装，增加一个四字节的 Tag 标签，在标签中描述该数据帧所属于的 VLAN。这样，当路由器或三层交换机的以太网接口接收到此帧时，就会根据其所携带的 Tag 标签来判断这个数据帧属于哪个 VLAN，并与接收接口所对应的 VLAN 进行比较。如果接收接口和数据帧属于同一个 VLAN，接口则接收此帧，否则将此帧丢弃。

3．干道协议

在以太网中为实现 VLAN 之间的相互通信，就需要用专门的协议封装或者加上标记（tag），以便接收设备能区分数据所属的 VLAN。VLAN 标识从逻辑上定义了，数据包使用哪种协议进行封装，而最常用到的是 IEEE 802.1q 协议和 CISCO 私有的 ISL 协议。IEEE 802.1q 协议用在不同的厂家生产的交换机之间，一个 IEEE 802.1q 干道端口同时支持加标签和未加标签的流量。

交换机的接口可以运行在接入模式（Access Mode）或者干道模式（Trunk Mode）。交换机接口所连接的链路也被相应地称为接入链路和 Trunk 链路。在接入模式下，接口属于且仅属

于一个 VLAN。而 Trunk（干道）是一种封装技术，它是一条点到点的链路，主要功能就是仅通过一条链路就实现多个 VLAN 的通信，如图 2-17 所示。

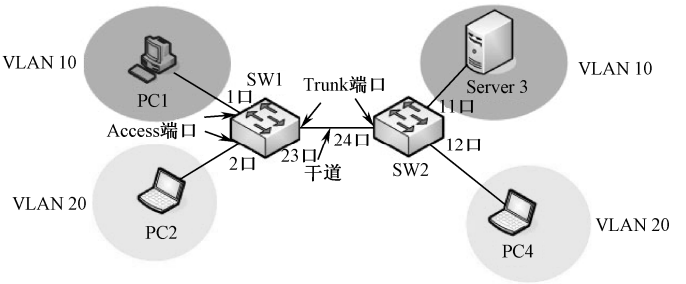


图 2-17　Trunk 干道实现多 VLAN 的通信

4．VLAN 配置

1）VLAN 配置命令

配置一个 VLAN 包括在交换机内创建一个 VLAN、为 VLAN 分配一定端口等。

（1）创建 VLAN

命令：Switch（config)#vlan *vlan-id*

说明：其中：*vlan-id* 是由管理员输入的要创建 VLAN 标号，范围在 1～4094。如果输入的是一个新的 VLAN id，则交换机会创建一个 VLAN，如果输入的是已经存在的 VLAN id，则修改相应的 VLAN。

案例：建立 VLAN10

```
Switch#config  ter          //进入全局配置模式
Switch(config)#vlan 10      //建立 VLAN10
```

（2）命名 VLAN

命令：Switch（config-vlan)#name *vlan-name*

说明：创建 VLAN 后，可以为该 VLAN 命名，以便日后维护方便，其中：*vlan-name* 是由管理员输入的 VLAN 名字。如果没有进行这一步，则交换机会自动为它起一个名字 VLAN ××××，其中××××是用 0 开头的四位 VLAN id 号，如，VLAN 0004 就是 VLAN 4 的默认名字。

案例：将 VLAN10 命名为 jiaoshi

```
Switch(config)#vlan 10                  //进入 VLAN10 配置模式
Switch(config-vlan)# name jiaoshi       //将 VLAN10 命名为 jiaoshi
```

（3）查看 VLAN 配置

命令：Switch#show vlan {id *vlan-id*}

说明：配置完 VLAN 后，维护过程中经常需要查看 VLAN 配置情况，确定某个 VLAN 包含哪些端口等，其中：*vlan-id* 是由管理员输入要查看的 VLAN 标号。*vlan-id* 是可选项，如没有输入，则查看交换机所有 VLAN 信息；如输入了 *vlan-id* 可选项，则只查看此 VLAN 的信息。

案例：显示交换机的 VLAN 信息

```
Switch>enable               //进入特权模式
```

```
Switch#show vlan            //显示交换机所有 VLAN 信息
Switch#show vlan id 10      //只显示 VLAN 10 的信息
```

（4）删除 VLAN

命令：Switch（config)#no vlan *vlan-id*

说明：在维护过程中，经常需要删除一些不使用的 VLAN，请注意在删除某一个 VLAN 时，要将这个 VLAN 包含的端口重新分配给其他 VLAN，否则将丢失这些端口。其中：*vlan-id* 是由管理员输入的要删除的 VLAN 标号。

案例：删除 VLAN10

```
Switch(config)#vlan 10      //进入 VLAN10 配置模式
Switch(config)#no vlan 10   //删除 VLAN 10
```

（5）进入交换机的单一物理端口

命令：Switch(config)# interface *fastEthernet id*

说明：进入端口状态下，才可以对该端口进行相应操作，如关闭端口、启动端口、设置端口速率和设置端口工作模式等，其中 id 为由管理员输入的要进入交换机的端口标号，如 0/1、0/2 等。

案例：进入端口 fa0/1

```
Switch#config                                   //进入全局配置模式
Switch(config)# interface fastEthernet  0/1     //进入端口 Fa 0/1 模式
```

（6）进入交换机的一组物理端口

命令：Switch(config)# interface range *port-rang*

说明：如果需要配置的端口数量较多，用前面介绍的方法一个一个单独配置比较麻烦，可以同时进入一组端口，对这组端口进行一次性配置，省时、省力、不易出错；其中：interface range 命令可以指定若干范围段，每个范围段可以使用逗号（,）隔开。*port-range* 为 fastethernet slot/{第一个 port} - {最后一个 port}；gigabitethernet slot/{第一个 port} - {最后一个 port}等。

案例：同时进入 Fa0/1 至 Fa0/5 及 Fa0/7、 Fa0/8 端口

```
Switch#config       //进入全局配置模式
Switch(config)#interface range fastEthernet 0/1-5,0/7-8   //同时进入 Fa0/1 至 Fa0/5 及 Fa0/7、 Fa0/8 端口模式
```

（7）设置交换机端口类型

命令：Switch(config-if)# switchport mode *access* | *trunk*

说明：交换机端口类型分为二层端口及三层端口，其中二层端口又分为 Access 类型和 Trunk 类型。通常，Aceess 类型连接计算机等终端设备，只能属于一个 VLAN；Trunk 类型用于交换机间连接，可以属于多个 VLAN。交换机默认端口类型为 Access 类型。

案例：设置 Fa0/1 端口类型为 access

```
Switch#config                                   //进入全局配置模式
Switch(config)#Interface Fa 0/1                 //进入 Fa0/1 端口模式
Switch(config-if)# switchport mode access       //设置 Fa0/1 端口类型为 access
```

（8）启动或关闭交换机端口

命令：Switch(config-if)# no shutdown | shutdown

说明：交换机端口可以通过命令启动或关闭，便于网络管理，其中：no shutdown 是启动该端口，Shutdown 是关闭该端口，默认状态为端口启动状态（no shutdown）

案例：启动端口 Fa0/1

```
Switch#config                          //进入全局配置模式
Switch(config)#Interface Fa 0/1        //进入 Fa0/1 端口模式
Switch(config-if)# no shutdown         //启动端口 Fa0/1
```

（9）分配 VLAN 端口

命令：Switch(config-if)# switchport access vlan *vlan-id*

说明：交换机创建 VLAN 后，必须将一个或多个端口分配到 VLAN 中，创建的 VLAN 才能发挥作用。在分配端口时可以一次分配一个端口，也可以一次分配多个端口到 VLAN 中。其中 *vlan-id* 是由管理员输入的要分配端口的 VLAN 标号。

案例：

```
Switch#config                                  //进入全局配置模式
Switch(config)#Interface Fa 0/1                //进入 Fa0/1 端口模式
Switch(config-if)# switchport mode access      //设置端口 Fa0/1 为 access 类型
Switch(config-if)# switchport access vlan 10   //将端口 Fa0/1 分配给 VLAN10
Switch(config-if)#end
Switch#show vlan                               //显示所有 VLAN
```

（10）配置 Native VLAN

命令：Switch(config-if)#switchport　trunk native vlan *vlan-id*

说明：为了提高交换机在 Trunk 类型端口的上传送效率，规定从 Native VLAN 中发送的数据帧不需要增加标签项，默认状态下 VLAN1 为 Native VLAN。若要设置 Native VLAN，链路两端 Native VLAN 的 VLAN id 必须相同，否则，将出现传送错误；其中 *vlan-id* 为设置为 Native VLAN 的 VLAN 标识。

案例：配置 Native VLAN 为 VLAN 10

```
Switch#config  //进入全局配置模式
Switch(config)#interface Fa0/24                          //进入 Fa0/24 端口模式
Switch(config-if)# switchport mode trunk                 //设置Fa0/24端口类型为Trunk
Switch(config-if)# switchport trunk native vlan 10       //设置交换机 Trunk 端口
Fa0/24 上收发 VLAN 10 的报文为 untag 报文
```

（11）Trunk 端口许可 VLAN 列表

命令：Switch(config-if)#switchport　trunk allowed　vlan *vlan-id*

说明：在网络工程中，为了安全起见，需要限制数据帧的任意传送，确保合法数据帧顺利传输，拒绝非法数据帧传输。其中：vlan-list 可以是一个 VLAN 或以 vlan n-vlan m 表示一组 VLAN，如 10～20；all 是许可 VLAN 列表包含所有 VLAN；add 表示将指定 VLAN 列表加入许可 VLAN 列表；remove 表示将指定 VLAN 列表从许可 VLAN 列表中删除；except 表示将除列出的 VLAN 列表外的所有 VLAN 加入许可 VLAN 列表；不能将 VLAN 1 从许可 VLAN 列表中移出。

案例：设置 fa0/24 口为 Trunk 模式，限制 VLAN 2 通过

```
Switch#config  //进入全局配置模式
Switch(config)#interface Fa0/24        //进入 Fa0/24 端口模式
Switch(config-if)# switchport mode trunk  //设置 Fa0/24 端口类型为 Trunk
Switch(config-if)# switchport trunk allowed  vlan remove 2//限制 VLAN 2 通过
```

5．路由器配置基础

1）路由器的外形结构

VLAN 间若需要相互访问，必须通过网络层实现，路由器（Router）是工作在 OSI 模式第三层的数据包转发设备，如图 2-18 所示。路由器的主要功能是检查数据包中与网络层相关的信息，然后根据某些选路规则对存储的数据包进行转发，这种转发称之为路由选择。

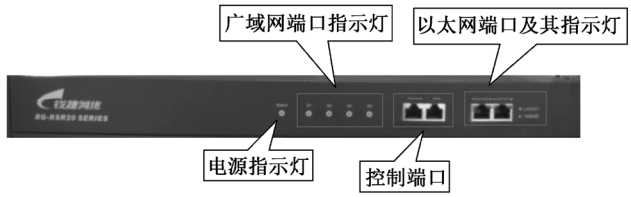


图 2-18　路由器前面板

6．路由器连接图

路由器的端口有以太网端口、串行端口、AUX 端口、Console 端口、子接口等；路由器子端口的逻辑特性与物理端口是一样的，我们如果给子端口配置 IP 地址，此地址作为子端口关联的 VLAN 的网关。同时，需要在各子端口上封装 802.1q 协议，使得路由端口能够识别接收到的 802.1q 数据帧。当 VLAN 中的设备需要将数据发送给其他子网时，会将数据帧发送到子端口，之后路由器通过查找路由表，根据数据中的目的 IP 地址决定数据从哪个子端口发出，从而到达相应的 VLAN 中，如图 2-19 所示，路由器的 Fa0/0 接口划分了 3 个子接口。

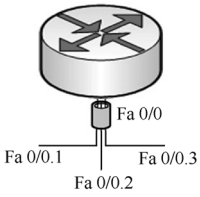


图 2-19　路由器的子接口

7．路由器工作原理

路由器可以连接多个网络或网段，对不同网络或网段间的数据信息进行“翻译”，以使它们能够相互读懂对方的数据，从而构成一个更大的网络。路由器通常会连接两个或多个 IP 子网或点对点协议标识的逻辑接口，如图 2-20 所示。

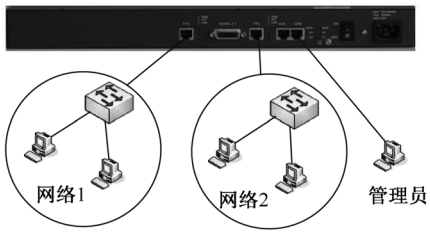


图 2-20　路由器连接两个 IP 子网

路由器根据收到的数据包中的网络层地址以及路由器内部维护的路由表，来决定输入接口以及下一跳路由器地址或主机地址，并重写链路层数据包头。路由器会应用路由表来反映当前的网络拓扑，通过与其他路由器交换路由信息来完成路由表的动态维护。路由器工作过程如图 2-21 所示。

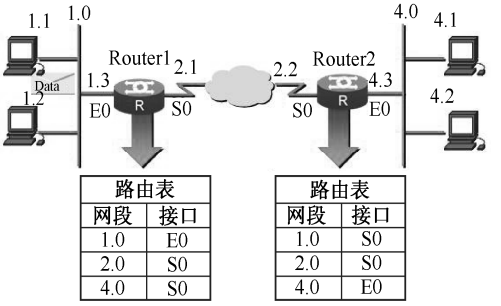


图 2-21　路由器工作过程

主机 1.1 要发送数据到 4.2

路由器 A 接收到数据，查看数据包中的目标地址为 4.2，查找路由表。

路由器 1 根据路由表转发数据到 S0 口。

路由器 2 接收到数据包，查看数据包的目标地址，并查找路由表。

路由器 2 根据路由表转发数据到 E0 口。

主机 4.2 接收到数据包

8．路由器登录方式

路由器同交换机一样，也有多种登录方式，常用的有超级终端和 Telnet 两种登录方式。超级终端方式登录是在路由器初次登录时必须使用的一种登录方式，不需要 IP 地址等设置，只要将登录计算机的 COM 口通过调试线与路由器 Console 端口连接，在计算机上进行必要的参数配置即可。特点是不需要网络即可登录，但管理员必须到达路由器所在机房才能登录。

Telnet 方式登录是通过连接计算机与路由器的网络进行的登录方式，在登录之前必须对路由器设置端口 IP 地址和登录密码等参数，特点是不需要进入路由器所在机房通过网络即可登录路由器。

9．路由器基本配置命令

路由器的配置模式与交换机的配置模式基本相同，有用户模式、特权模式、全局配置模式、接口配置模式、VLAN 配置模式等，同时直接使用【Tab】键自动补齐命令。路由器的基本配置的命令同交换机基本相同，用户也可以输入“？”来获得提示与帮助。一台路由器的基本配置和交换机基本相同，包括以下方面：

（1）配置路由器名字

命令：Router (config)#hostname name

说明：在网络设备参数配置及日后运营维护路由器系统名称都非常必要，修改时也是立即生效。其中：name 为路由器的主机名。

注意：使用该命令的 no 选项将该设置恢复为默认值，如 MyRouter (config)#no hostname。

案例：将路由器系统名称修改为 RouterA

```
Router (config)# hostname RouterA //路由器系统名称修改为 RouterA
```

```
RouterA (config)#
```

（2）配置路由器端口 IP 地址

命令：Router (config-if)# IP address *ip-address sub-mask*

说明：路由器端口 IP 地址是必须配置的，路由器与交换机不同，路由器通过端口进行数据包转发，端口不配置有效的 IP 地址不能正常工作，其中：ip-address 为需要设置的 IP 地址，*sub-mask* 为 IP 地址的子网掩码。

案例：配置 fa0/0 的 IP 地址为 192.168.0.1

```
Router (config)# Interface Fasterethernet 0/0 //进入端口 FastEthernet0/0
Router (config-if)# ip address 192.168.0.1 255.255.255.0 //配置端口 FastEthernet0/0
的 IP 地址为 192.168.0.1
Router (config-if)# no shutdown    //开启端口 FastEthernet0/0
Router (config--if)#end
Router #show interfastether 0/0    //显示端口 FastEthernet0/0 状态
```

（3）配置子接口命令

命令：Route(config)# interface fastethernet *slot-number*

/interface-number.subinterface-number

说明：其中：*slot-number* /*interface-number* 为槽号/物理端口序号，*subinterface-number* 为子端口在该物理端口上的序号，注意二者之间由标号“.”连接。

案例：配置 fastEthernet 0/0.1 的子接口，并分配 IP 地址。

```
Route(config)#interface fastEthernet 0/0.1//进入子端口 Fa0/0.1
```

（4）配置子接口封装 802.1q

命令：Route(config-subif)#encapsulation dot1q *vlanid*

说明：为路由器的子接口封装 802.1q，主要是为了 VLAN 通信。其中：*vlanid* 为虚拟局域网 VLAN 的 ID，取值范围为 1～4094 的整数。

案例：配置 fastEthernet 0/0.2 的子接口，封装 802.1q

```
Route(config)#interface fastEthernet 0/0.2            //进入子端口 Fa0/0.2
Route(config-subif)# encapsulation dot1q 20           //封装 802.1Q,指定 Fa0/0.2
属于 VLAN 20
Route(config-subif)#ip addresss 192.168.10. 1 255.255.255.0 //其他子端口参考配置
Route(config-subif)#no shutdown                       //激活端口
```

（5）设置路由器远程登录密码

命令：具体命令如表 2-3 所示。

表 2-3　配置路由器远程登录密码命令格式

命　令	说　明
Router(config)#line vty *first-line last-line*	其中：*first-line* 为开始线路编号，*last-line* 为结束线路编号
Router(config-line)#password *password-value*	其中：*password-value* 为登录密码
Router (config-line)#login	

说明：设置路由器的远程登录密码，有利用保护路由器的设备安全。

案例：设置路由器远程登录密码 123456

```
Router #config                          //进入全局配置模式
Router (config)#line vty 0 4            //其中：0 表示线路 line0，4 表示线路 line4，此命令表示
                                        //允许 line0 到 line4 共 5 个客户同时登录
Router (config-line)#password 123456    //设置登录密码为 123456
Router (config-line)#login              //启动 line 线路密码保护
```

（6）设置路由器特权密码

命令：格式如表 2-4 所示。

表 2-4　命令格式及说明

命 令 格 式	说　明
Router(config)#enable secret [*level level*] {*encryption-type encrypted-password*}	其中： *level level* 为口令应用到的路由器的管理级别。可以设置 0 到 15 共 16 个级别，如果不指明级别则默认为 15 级。Level=15 为特权密码设置。 *encryption-type* 为加密类型。0 表示用明文输入口令，5 表示用密文输入口令。 *encrypted-password* 为输入的口令。如果加密类型为 0，则口令是以明文形式输入；如果加密类型为 5，则口令是以密文形式输入。 注意：使用该命令的 no 选项将禁止该级别。如：no enable secret [level level]

说明：密码分为特权密码和远程登录密码，其中：特权密码是指从用户模式（Switch>）到特权模式（Switch#）时使用的密码。

案例：配置路由器特权密码 123456

```
Router #config //进入全局配置模式
Router(config)# enable secret level 16 0 123456     //设置路由器特权密码为 123456，
                                                     //明文方式
```

（7）其他命令

其他命令见表 2-5。

表 2-5　其他命令

范　例	说　明
Router# show　version	显示系统、版本信息
Router# show　running-config	显示 RAM 里当前生效的配置
Router# show　ip route	显示路由表
Router# show interface FastEthernet0/0	显示接口 FastEthernet0/0 信息
Router#copy running-config startup-config	将配置保存到 Flash 中 也可以直接输入 wirte 保存
Router(config)# del config.text	删除当前的配置，恢复默认值
Router# reload	将交换机重新启动

项目实施

任务一　实现按部门划分网络

任务描述

商畅数码有限公司是一家新成立的小型企业，公司有行政部、研发部、财务部和销售部 4

个部门共计 21 名员工，现在网络管理员小李要进行公司局域网的组建，要求公司的网络能够实现按部门进行划分。

网络拓扑

家庭网络拓扑结构如图 2-22 所示。

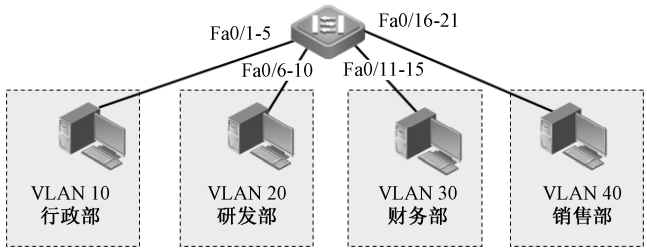


图 2-22　家庭网络拓扑结构图

任务目标

制作双绞线 N 条，连接计算机和交换机后，进行交换机的相关配置实现 VLAN 的划分。

设备清单

交换机 1 台、双绞线 N 条。

工作过程

步骤一：制作双绞线，并连接设备

略（详细见项目一的制作过程）。

步骤二：进行 IP 地址规划

IP 地址表见表 2-6。

表 2-6　IP 地址表

设　备	VLAN	IP	接　口
行政部计算机	VLAN10	192.168.10.2/24	Fa0/1～5
研发部计算机	VLAN 20	192.168.20.2/24	Fa0/6～10
财务部计算机	VLAN 30	192.168.30.2/24	Fa0/11～15
销售部计算机	VLAN 40	192.168.40.2/24	Fa0/16～21

步骤三：配置交换机

第 1 步：创建 VLAN。配置命令如下：

```
Switch>enable                          //进入特权配置模式
Switch#config ter                      //进入全局配置模式
Switch(config)#vlan 10                 //创建 VLAN10
Switch(config-vlan)#name  XZB          //VLAN 名字为 XZB
Switch(config-vlan)#exit               //返回全局配置模式
Switch(config)#vlan 20
Switch(config-vlan)#name  YFB
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#vlan 30
```

```
Switch(config-vlan)#name  CWB
Switch(config-vlan)#exit
Switch(config)#vlan 40
Switch(config-vlan)#name  XSB
Switch(config-vlan)#exit
```

第 2 步：分配交换机端口到 VLAN。将交换机端口 Fa0/1、Fa0/2 分配到 VLAN10 中，将交换机端口 Fa0/11、Fa0/12 分配到 VLAN20 中。配置命令如下：

```
Switch(config)#interface range fastethernet 0/1-5   //进入 fa0/1-5 端口
Switch(config-if-range)#switch mode access          //设置端口的工作模式为 access
Switch(config-if-range)#switch access vlan 10       //将端口划分给 vlan 10
Switch(config-if-range)#exit                        //返回全局配置模式
Switch(config)#interface range fastethernet 0/6-10
Switch(config-if-range)#switch mode access
Switch(config-if-range)#switch access vlan 20
Switch(config-if-range)#exit
Switch(config)#interface range fastethernet 0/11-15
Switch(config-if-range)#switch mode access
Switch(config-if-range)#switch access vlan 30
Switch(config-if-range)#exit
Switch(config)#interface range fastethernet 0/16-21
Switch(config-if-range)#switch mode access
Switch(config-if-range)#switch access vlan 40
Switch(config-if-range)#exit
Switch(config)# exit
Switch#write   \\保存配置
```

第 3 步：查看交换机 VLAN 信息。

```
Switch#show vlan
VLAN Name                              Status    Ports
---- --------------------------------    ---------
1    default                           active    Fa0/22, Fa0/23, Fa0/24
10   XZB                               active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5
20   YEB                               active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10
30   CWB                               active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15
40   XSB                               active    Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21
.....
```

项目测试

在行政部配置两台计算机的 IP 地址，A 机的 IP 地址为 192.168.10.2/24，B 机的 IP 地址为 192.168.10.3/24，使用 ping 命令测试 B 机到 A 机的数据连通性，发现在同一 VLAN

的计算机可以通信，而行政部的计算机不能与其他部门的计算机实现通信，这样就实现了部门间网络的二层隔离。如图 2-23 所示。

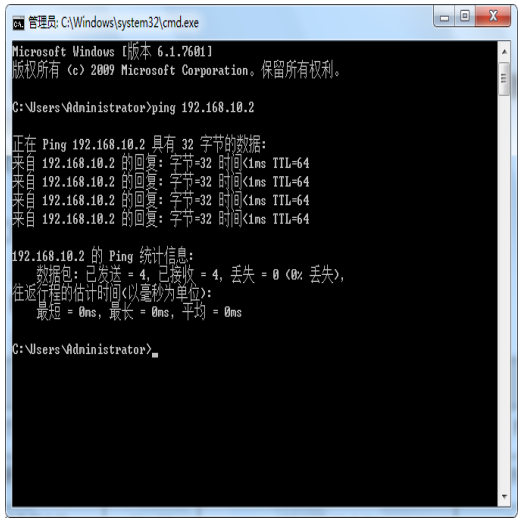


图 2-23　同一个 VLAN 的计算机能够连通

任务二　实现部门网络间的通信

任务描述

网络管理员小李已经配置了交换机的 VLAN 功能，实现了部门间的网络二层隔离，为了使公司内所有的计算机都可以相互访问，网络管理员小李通过配置路由器的子接口来实现不同部门间计算机的通信，即路由器的单臂路由功能。

网络拓扑

其网络拓扑图如图 2-24 所示。

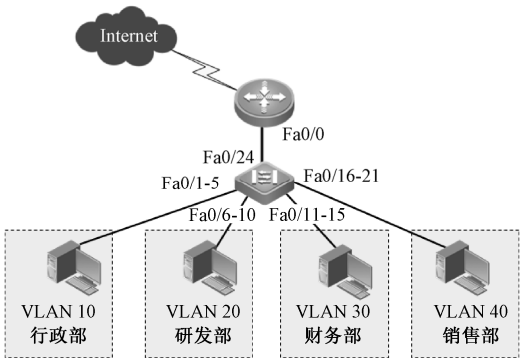


图 2-24　网络拓扑图

任务目标

配置路由器的子接口和交换机的 Trunk 口实现部门之间计算机的通信。

设备清单

路由器 1 台、交换机 1 台、双绞线 N 条。

工作过程

步骤一：连接路由器与交换机

步骤二：配置交换机

```
Switch>enable
Switch#config t
Switch(config)#interface fa0/24                    //进入 fa0/24 端口
Switch(config-if)#switchport mode trunk            //设置端口的工作模式为 trunk
Switch(config-if)#switchport trunk allowed vlan all   //设置 Trunk 允许所有 vlan 通过
Switch(config-if)#exit
Switch(config)#exit
Switch#write                                       //保存配置
Building configuration...
[OK]
```

步骤三：配置路由器

```
Router>enable                          //进入特权配置模式
Router#config ter                      //进入全局配置模式
Router(config)#interface fa0/0.1   //进入子接口 fa0/0.1
Router(config-subif)#encapsulation dot1q 10  //封装 802.1Q，指定 Fa0/0.1 属于 VLAN 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0 //设置子接口的 IP 地址
Router(config-subif)#no shutdown   //激活端口
Router(config-subif)#exit
Router(config)#interface fa0/0.2
Router(config-subif)#encapsulation dot1q 20 //封装 802.1Q，指定 Fa0/0.2 属于 VLAN 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0 //设置子接口 IP 地址
Router(config-subif)#no shutdown
Router(config-subif)#exit
Router(config)#interface fa0/0.3
Router(config-subif)#encapsulation dot1q 30
Router(config-subif)#ip address 192.168.30.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fa0/0.4
Router(config-subif)#encapsulation dot1Q 40
Router(config-subif)#ip address 192.168.40.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fa0/0
Router(config-if)#no shutdown      //激活端口
Router(config-if)#exit
Router(config)#exit
Router#show ip route               //显示路由表
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
```

```
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
C    192.168.10.0/24 is directly connected, FastEthernet0/0.1
C    192.168.20.0/24 is directly connected, FastEthernet0/0.2
C    192.168.30.0/24 is directly connected, FastEthernet0/0.3
C    192.168.40.0/24 is directly connected, FastEthernet0/0.4
Router#write  \\保存配置
Building configuration...
[OK]
```

注意：如要实现连接因特网，还需要做 NAT 配置，NAT 配置将在项目六中阐述。

项目测试

步骤一：测试部门计算机到网关的连通性，如行政部 VLAN10 中的 PC 网关应该是 192.168.10.1。如图 2-25 所示。

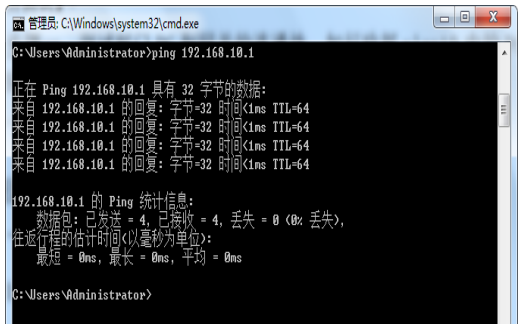


图 2-25　测试与网关的连通性

步骤二：测试部门之间计算机的连通性，如测试行政部 VLAN 10 的计算机与研发部计算机间的连通性，如图 2-26 所示。

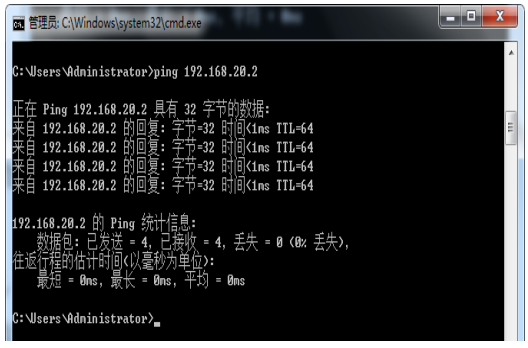


图 2-26　测试部门间计算机的连通性

认证测试

一、选择题

1．下列哪些命令不可以保存交换机的配置信息（　　）。

A．Write　　B．copy running-config startup-config

C．Write memory　　D．copy startup-config running-connfig

2．下列哪条命令是接口配置模式（　　）。

A．>　　B．#　　C．(config)#　　D．(config-if)#

3．下列哪条命令是显示详细计算机网络参数的命令（　　）。

A．ipconfig　　B．show interface Ethernet 0/0/1

C．ipconfig/all　　D．show running-config

4．当我们在交换机配置时需要查找当前命令时需要输入（　　）。

A．?　　B．#　　C．help　　D．/?

5．当要使一个 VLAN 跨交换机时，需要（　　）特性支持。

A．用三层端口连接两台交换机　　B．用 Trunk 端口连接两台交换机

C．用路由器连接两台交换机　　D．两台交换机上 VLAN 的配置必须相同

6．局域网内使用 VLAN 所带来的好处是（　　）。

A．可以简化网络管理的配置工作量

B．广播可以得到控制

C．局域网的容量可以扩大

D．可以通过部门等将用户分组而打破物理位置的限制

7．下面（　　）命令可以正确地为 VLAN10 定义一个子端口。

A．router(config-if)#encapsulation dot1q 10

B．router(config-if)#encapsulation dot1q　vlan 10

C．router(config-subif)#encapsulation dot1q 10

D．router(config-subif)# encapsulation dot1q　vlan 10

二、简答题

1．简述什么是 VLAN 及它的优点？

2．简述交换机带外管理的步骤？

3．简述路由器的工作原理？

4．描述单臂路由的工作过程及特点？

5．描述配置单臂路由的命令及步骤？

项目三　富华酒店网络配置与管理

项目背景

富华大酒店是一所五星级酒店，位于广州天河区，酒店楼高 31 层，建筑面积四万多平方米，拥有各类客房 400 余间，设有 5 个特色餐厅和一个超大厅堂的饮食场所，另外设有夜总会、桌球室、保龄球场、游泳池等娱乐场所，还有两间多功能厅酒店会议中心。为提高服务质量，酒店的王总经理决定进行网络的升级改造，要求酒店所有办公计算机都连入网络，并且要求每个客房实现网线直接接入即可上网；在餐厅、桌球室、保龄球场等娱乐场所和会议厅实现无线网络接入，客人在酒店任何场所都可以用手机或 iPad 实现上网，力争打造一个数字信息化的多功能酒店。

富华大酒店如图 3-1 所示。

图 3-1　富华大酒店

项目分析

分析一：王总经理要求将所有计算机接入网络，部分场所要配备无线网络，实现网络的互连互通。

分析二：王总经理要求客户的计算机能自动获取到 IP 地址，自动接入酒店网络。

项目方案

富华大酒店的网络属于中型网络，中型网络范围比较大，需要连接的计算机较多，就需要使用更多的网络设备。富华大酒店有近千个信息点，此时应选用三层交换机作为大楼网络的核心设备。酒店的客户流动性很大，管理比较困难，需要在网络用到 DHCP 服务器，来实现用户自动获取 IP 地址，客户只需要接上网线就可以上网了。其网络拓扑结构如图 3-2 所示。

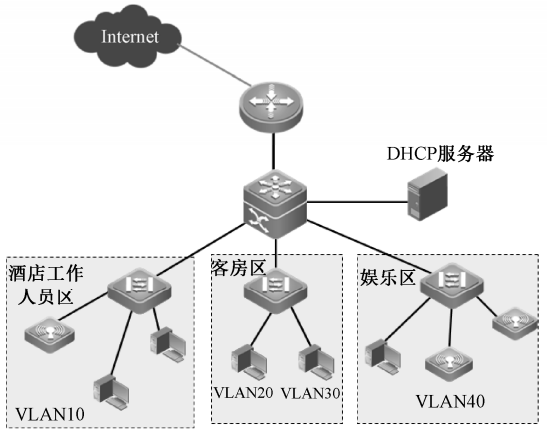


图 3-2　网络拓扑图

知识准备

1．三层交换机配置

1）三层交换机概述

以太网 VLAN 技术在网络中得到了大量的应用，而各个不同 VLAN 间的通信都要经过路由器来完成转发，随着网络间互访的不断增加。单纯使用路由器来实现网络间访问，不但由于端口数量有限，而且路由速度较慢，从而限制了网络的规模和访问速度。基于这种情况，三层交换机便应运而生，三层交换机就是具有部分路由器功能的交换机，专为网络层设计的，接口类型简单，拥有很强的二层包处理能力，非常适用于大型局域网内的数据路由与交换，它既可以工作在协议第三层替代或部分完成传统路由器的功能，同时又具有几乎第二层交换的速度，三层交换机最重要的目的是加快中大型局域网内部的数据交换，所具有的路由功能也是为这个目的服务的，能够做到一次路由，多次转发，如图 3-3 所示。

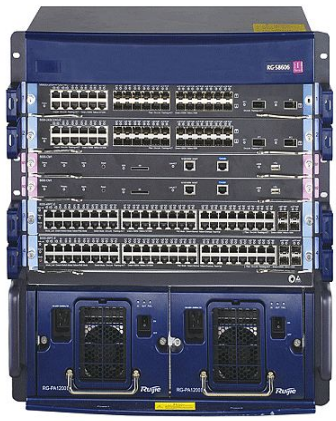


图 3-3　企业三层核心路由器

三层交换机除了优秀的性能之外，还具有一些传统二层交换机没有的特性，具有高可扩充性、高性价比、内置安全机制、适合多媒体传输、并且还具有计费功能等。现在三层交换机已经广泛应用在校园网、城域网、智能小区网络等场所。

2）交换虚拟接口

SVI（Switch Virtual interface）是交换虚拟接口，用来实现三层交换的逻辑接口。 SVI 可以作为设备的管理接口，通过该管理接口来管理网络设备。您也可以创建 SVI 为一个网关接口，就相当于是对应各个 VLAN 的虚拟子接口，可用于 3 层设备中跨 VLAN 之间的路由。创建一个 SVI 很简单，可通过 Interface Vlan SVI 接口配置命令来创建 SVI，然后给 SVI 分配 IP 地址来建立 VLAN 之间的路由。

如图 3-3 所示，VLAN20 的主机可直接互相通信，无需通过三层设备的路由，若 VLAN20 内的主机 PC1 想和 VLAN30 内的主机 PC4 通信，必须通过 VLAN20 对应的 SVI1 和 VLAN30 对应的 SVI 才能实现。

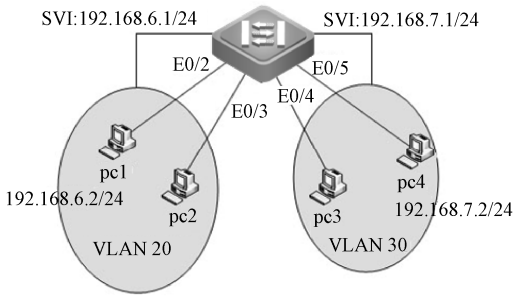


图 3-4 SVI 示意图

3）三层交换机配置

（1）三层交换机 SVI 配置

三层交换机的配置与二层交换机配置的基本命令相同，不同的是二层交换机只有一个 VLAN1 的虚拟逻辑端口作为交换机管理端口，而三层交换机可以为每个 VLAN 都分配一个虚拟端口，给每个虚拟端口都配置一个 IP 地址。

① 进入 SVI 命令

命令：Switch(config)#interface vlan id

说明：其中：id 为管理员要配置的交换机虚拟端口 IP 地址对应的 VLAN 标号，注意，虚拟端口与物理端口具有同样功能，通常虚拟端口作为该 VLAN 内主机的网关。

案例：进入 VLAN10 的虚拟端口（SVI）

```
Switch#config  //进入全局配置模式
Switch(config)#ip routing  //默认状态是开启的
Switch(config)#interface vlan 10  //进入 VLAN10 的虚拟端口（SVI）
```

②设置虚拟端口 IP 地址

命令：Switch(config-if)# ip address *ip-address network-mask*

说明：其中：*ip-address* 为 32 位 IP 地址，8 位一组，以十进制数方式表示，组之间用点隔开。*network-mask* 为 32 位网络掩码，“1”表示掩码位，“0”表示主机位。每 8 位一组，以十进制数方式表示，组之间用点隔开。

注意：此地址为相应 VLAN 中计算机的网关地址。

案例：设置 VLAN 虚拟端口的 IP 地址

```
Switch#config  //进入全局配置模式
Switch(config)#interface vlan 10  //进入 VLAN10 虚拟端口模式
Switch(config-if) #ip address 192.168.10.1 255.255.255.0  //设置端口 IP 地址
```

```
Switch(config-if)# no shutdown  //启动 VLAN10 的虚拟端口
```

（2）配置实例

以图 3-2 为例创建 VLAN20 和 VLAN30 并通过 VLAN20 对应的 SVI1 和 VLAN30 对应的 SVI2 实现 PC1 与 PC4 通信。

第 1 步：创建 VLAN20 并划分端口 e0/0/2 与 e0/0/3。

```
switch(config)#vlan 20
switch(config-vlan)#switchport interface Ethernet 0/0/2～3
switch(config-vlan)#exit
```

第 2 步：创建 VLAN30 并划分端口 e0/0/4 与 e0/0/5。

```
switch(config)#vlan 30
switch(config-vlan)#switchport interface ethernet 0/0/4-5
switch(config-vlan)#exit
```

第 3 步：配置 VLAN20 对应的 SVI。

```
switch(config)#interface vlan 20
switch(config-If-Vlan)# ip address 192.168.6.1 255.255.255.0
switch(config-If)#no shutdown
switch(config-If)#exit
```

第 4 步：配置 VLAN30 对应的 SVI。

```
switch(config)#interface vlan 30
switch(config-If)# ip address 192.168.7.1 255.255.255.0
switch(config-If)#no shutdown
switch(config-If)#exit
```

第 5 步：测试。

在 PC1 上运行 ping 命令测试，如图 3-5 所示。

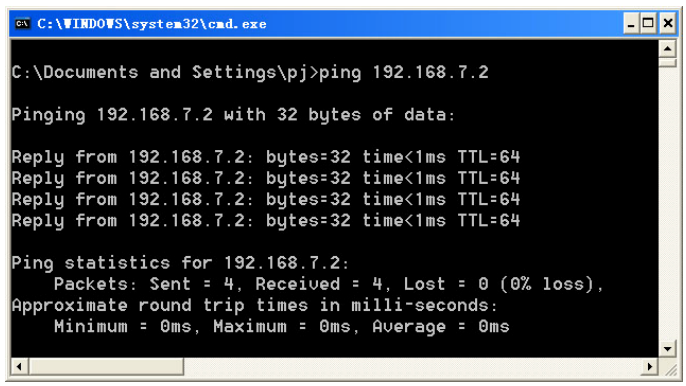


图 3-5　PC1 上 ping 命令测试结果

2．静态路由配置

1）什么是路由

路由是指在 OSI 参考模型第三层的设备，路由器或三层交换机从一个接口上收到数据包，

根据数据包的目的地址进行定向并转发到另一个接口的过程。

2）路由表

路由是把信息从源传输到目的地的行为，而路由表是在路由器中维护的路由条目，路由器根据路由表做路径选择。路由表就像一张地图，标记着各种路线，信息包就依靠路由表中的路线指引来到达目的地，路由条目就好像是路标，如表 3-1 所示，路由器当读到 IP 包的目的地址为 192.168.1.0，则将数据从 E0 端口发送出去。

表 3-1　简单路由表

网　　段	接　　口
192.168.1.0	E0
192.168.2.0	S0
192.168.3.0	S0

3．路由信息获取方式

路由器为了实现数据转发就必须要拥有路由信息。路由器的路由信息主要通过以下几种方式获得：

（1）直连路由

路由器自动添加和直连网络的路由。由于直连路由反映的接口所直接连接的网络非“二手”信息，因此其可信程序是比较高的。当在路由器上配置了接口的 IP 地址，并且接口状态为 UP 的时候，路由表中就出现直连路由项。如图 3-6 所示，路由器 R1 所连接的两个网段且接口状态 UP 后，路由器自动添加 192.168.1.0/24 和 10.0.00/8 两个网段在路由表中。

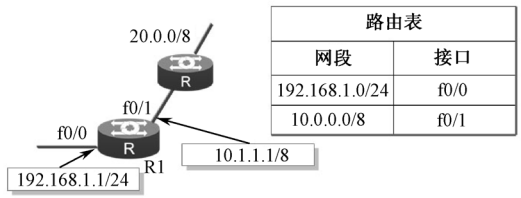


图 3-6　直连路由

（2）静态路由

静态路由是由管理员手工配置的，它不会自动跟随网络拓扑的变化而变化。静态路由不会占用路由器 CPU 和 RAM，也不占用线路的带宽，一般适用于结构比较简单的网络，如图 3-7 所示。

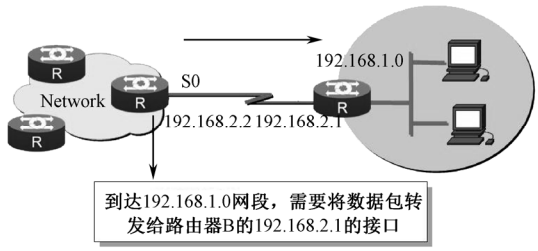


图 3-7　静态路由

（3）动态路由

通过各路由器之间连接的网络，利用路由协议动态地相互交换路由信息。通过这种交换，网络上的路由器就会知道网络中其他网端的信息，从而动态生成和维护相应的路由表。当目标网络有多条路径时，其中一条路径失效时，动态路由会自动切换到另一条路径。常用的动态路由协议有 RIP 和 OSPF 两种。

（4）默认路由

默认路由是静态路由的一种特殊应用，当路由器在路由表中找不到目标网络的路由条目时，路由器把请求转发到默认路由接口。在所有路由类型中，默认路由的优先级最低，适用环境一般应用在只有一个出口的末端网络中或作为其他路由的补充。末梢网络一般只有一个网络出口，可以在末梢网络的三层路由设备上，使用默认路由来发送那些网络中没有包含在路由表中的数据包，如图 3-8 所示。

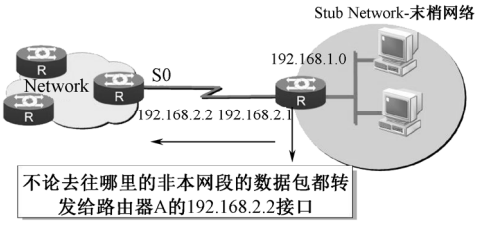


图 3-8　末梢网络使用默认路由

4．静态路由配置命令

1）静态路由特点

（1）静态路由是指由网络管理员手工配置的路由信息，是单向的。

（2）当网络的拓扑结构或链路的状态发生变化时，网络管理员需要手工去修改路由表中相关的静态路由信息。静态路由信息在缺省情况下是私有的，不会传递给其他的路由器。

（3）静态路由一般适用于比较简单的网络环境，在这样的环境中，网络管理员易于清楚地了解网络的拓扑结构，便于设置正确的路由信息。

2）配置静态路由

在非直连的网络当中，可以在三层交换机或路由器上，手工配置指向非直连网络的路由信息。

（1）静态路由配置命令

命令：Switch(config)#ip route *network net-mask* {*ip-address* | *interface* [*ip-address*]} [*distance*]

说明：network 为目标网络；net-mask 为网络掩码；ip-address 为到达该网络的下一跳 IP 地址；interface（可选）为到达该网络的数据包转发端口；distance（可选）为设置管理距离值，静态路由默认管理距离值是 1，该命令的 no 形式用来删除已配置的静态路由.

案例：配置 172.18.10.0 的路由下一跳地址为：10.1.1.1

```
Switch#config
Switch(config)#ip route 172.18.10.0 255.255.255.0 10.1.1.1
```

（2）显示路由表

命令：Switch # show ip route {[network [mask]]

说明：network：（可选）只显示该网络路由；mask：（可选）网络的掩码。

案例：显示路由表

```
Switch>enable
Switch #show ip route
```

（3）启动三层交换机的 IP 路由功能

命令：Switch(config)#ip routing

说明：显示三层交换机路由表，使用 No ip routing 命令关闭 IP 路由功能。

案例：启动三层交换机的路由功能。

```
Switch#configuration
Switch(config)#ip routing
```

（4）设置三层交换机的路由端口

命令：Switch(config-if)# no switchport

说明：使用 switchport 命令设置三层交换机端口为二层端口。

案例：将交换机的 Fa0/24 端口配置为路由口。

```
Switch#configuration   //进入全局配置模式
Switch(config)#Interface fastethernet 0/24//进入 Fa0/24 端口模式
Switch(config-if)# no switchport   //将 Fa0/24 端口配置为路由口
Switch(config-if)#ip address 192.178.100.1 255.255.255.0   //配置 Fa0/24 端口 IP
//地址为 192.178. 100.1/24
Switch(config-if)#no shutdown
```

（5）配置默认路由

命令：Switch(config)#ip route 0.0.0.0 0.0.0.0 {ip-address | interface [ip-address]} [distance]

说明：0.0.0.0 0.0.0.0 的目标网络和子网掩码，表示目标为所有网络； ip-address 为到达该网络的下一跳 IP 地址；interface（可选）为到达该网络的数据包转发端口；distance（可选）为设置管理距离值，该命令的 no 形式用来删除已配置的静态路由。

案例：配置一条默认路由，下一跳地址为：10.1.1.2

```
Switch#config  //进入全局配置模式
Switch(config)#ip route 0.0.0.0 0.0.0.0  10.1.1.2 //在末梢网络中不论去往哪里的非
//本网段的数据包都转发给下一跳地址 10.1.1.2
```

5．DHCP 配置

1）DHCP 服务器工作原理

动态主机配置协议（Dynamic Host Configuration Protocol，DHCP）是一种在网络中常用动态配置网络参数的技术，代替网络管理员手工配置及维护 IP 地址工作。DHCP 使用 UDP 传输协议，使用 67、68 端口号，从 DHCP 客户端到达 DHCP 服务器的报文使用目的端口号 67，从 DHCP 服务器到达 DHCP 客户端报文使用源端口号 68。

DHCP 工作过程如下。

（1）发现阶段。发现阶段是 DHCP 客户端寻址 DHCP 服务器阶段。在这期间，由于 DHCP 客户端还没有可用的 IP 地址，那么 DHCP 客户端使用目的 IP 地址 255.255.255.255 和目的 MAC

地址 FFFF-FFFF-FFFF 以广播方式发送 DHCPDISCOVER 发现报文。网络中的每一台主机（包括所有客户端主机及 DHCP 服务器）都会收到这个发现报文，如图 3-9 所示。

（2）提供阶段。提供阶段是 DHCP 服务器提供 IP 地址的阶段。DHCP 服务器收到 DHCPDISCOVER 报文后，从 DHCP 服务器中尚未分配的 IP 地址中选出一个 IP 地址分配给 DHCP 客户端，并通过向 DHCP 客户端发送一个包含待分配的 IP 地址和其他网络参数的 DHCPOFFER 提供报文作为对客户端的响应，如图 3-10 所示。

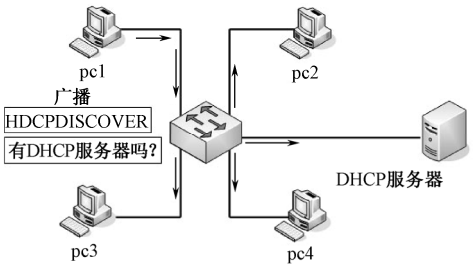


图 3-9　发现阶段

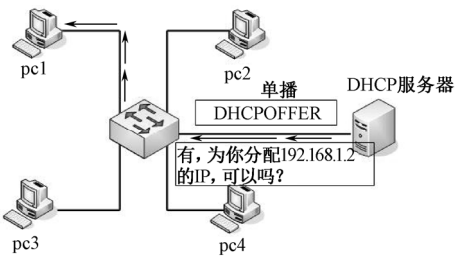


图 3-10　提供阶段

（3）选择阶段。选择阶段是 DHCP 客户端对 DHCP 服务器提供的 IP 地址进行选择的阶段。如果网络中有多台 DHCP 服务器同时提供 DHCP 服务，DHCP 客户端只接受第一个收到的 DHCPOFFER 报文，然后，DHCP 客户端以广播方式发送 DHCPREQUEST 请求报文作为对 DHCP 服务器的响应，如图 3-11 所示。

（4）确认阶段。确认阶段是 DHCP 服务器向客户端确认所提供 IP 地址可以使用的阶段。当 DHCP 服务器收到 DHCP 客户端的 DHCPREQUEST 请求报文后，向客户端发送一个包含所提供 IP 地址及其他网络参数的 DHCPACK 确认报文，表明客户端可以使用所提供的网络参数。DHCP 客户端收到 DHCPACK 确认报文后，开始使用 IP 地址及其他网络参数进行网络配置，如图 3-12 所示。

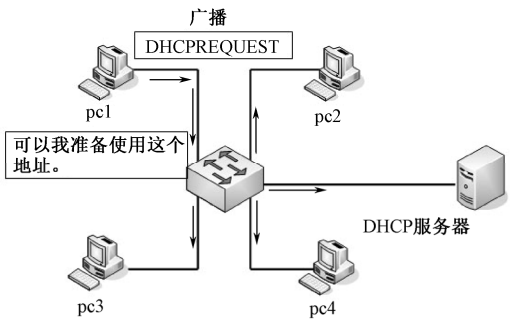


图 3-11　选择阶段

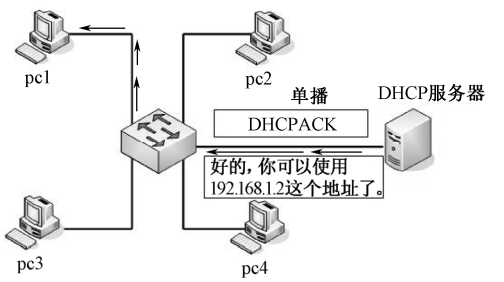


图 3-12　确认阶段

另外除了以上四个阶段外，还有一个 IP 租约更新的阶段。当 DHCP 客户机租期达 50%，重新更新租约，客户机发送 DHCPREQUEST 包；当租约达到 87.5%时，进入重新申请状态，客户机发送 DHCPDISCOVER 包；客户机可使用 ipconfig /renew 命令，向 DHCP 服务器发送 DHCPREQUEST 包，如果 DHCP 服务器没有响应，客户机将继续使用当前的配置直到租期达到 100%后，必须放弃这个 IP 地址。

6．配置交换机作为 DHCP 服务器

（1）启用 DHCP 服务器

命令：service dhcp

no service dhcp

说明：在全局配置模式下，启用 DHCP 服务器和 DHCP 中继代理功能。

举例：开启交换机的 DHCP 服务器或中继代理功能。

```
Switch(config)# service dhcp
```

（2）创建/删除 DHCP 地址池

命令：ip dhcp pool <name>

no ip dhcp pool <name>

说明：在全局配置模式下，配置 DHCP 地址池，进入 DHCP 地址池模式；本命令的 no 操作为删除该地址池。<name>为地址池名，最长不超过 255 个字符。

举例：定义一个地址池，取名 jackson。

```
Switch(config)#ip dhcp pool jackson
Switch(dhcp-config)#
```

（3）设置 DHCP 分配的网段

命令：network-address <network-number> [<mask> | <prefix-length>]

说明：在 DHCP 地址池配置模式下，配置 DHCP 分配网段；<network-number>为网络号码，<mask>为掩码，均为点分十进制格式，<prefix-length>为用前缀表示法，如掩码 255.255.255.0，用前缀法表示为 24。

举例：设置 DHCP 分配的网段为 192.168.1.0/24

```
Switch (dhcp-config)#network-address 192.168.1.0 24
```

（4）设置 DHCP 分配的缺省网关

命令：default-router <address1>[<address2>[…<address8>]]

说明：在 DHCP 地址池配置模式下，配置 DHCP 分配的缺省网关；address1…address8 为 IP 地址，均为点分十进制格式。

举例：设置 DHCP 分配的缺省网关为 192.168.1.1

```
Switch (dhcp- config)#default-router 192.168.1.1
```

（5）设置 DHCP 分配的 DNS 地址

命令：dns-server <address1>[<address2>[…<address8>]]

说明：在 DHCP 地址池配置模式下，配置 DHCP 分配的 DNS 地址，address1…address8 为 IP 地址，均为点分十进制格式。

举例：设置 DHCP 分配的 DNS 为 202.96.128.68

```
Switch (dhcp-config)#dns-server 202.96.128.68
```

（6）设置客户端域名

命令：domain-name <domain-name>

说明：在 DHCP 地址池配置模式下，设置客户端域名；<domain-name> 指客户端的后缀

域名字符串。

举例：配置客户端域名为 jackson.com

```
Switch (dhcp-config)# domain-name jackson.com
```

（7）设置 WIN 服务器地址

命令：netbios-name-server <address1>[<address2>[…<address8>]]

说明：在 DHCP 地址池配置模式下，设置 WIN 服务器地址；address1…address8 为 IP 地址，均为点分十进制格式。

举例：设置 WIN 服务器地址为：192.168.1.100

```
Switch (dhcp-config)# netbios-name-server 192.168.1.100
```

（8）设置客户 WIN 结点类型

命令：netbios-node-type <type>

说明：在 DHCP 地址池配置模式下，设置客户 WIN 结点类型；<type>为结点类型。

举例：设置客户 WIN 结点类型为复合型

```
Switch (dhcp-config)#netbios-node-type h-node
```

（9）设置 DHCP 分配的租期

命令：lease { [<days>] [<hours>][<minutes>] | infinite }

说明：在 DHCP 地址池配置模式下，配置 DHCP 分配的租期；<days>为天数，取值范围为 0～365，<hours>为小时数，取值范围为 0～23，<minutes>为分数，取值范围为 0～59；infinite 为永久使用。

举例：设置 DHCP 分配的租期为 8 小时

```
Switch (dhcp-config)#lease 0 8
```

（10）设置 DHCP 地址池中禁止分配的地址

命令：ip dhcp excluded-address <low-address> [<high-address>]

说明：在全局配置模式，设置 DHCP 地址池中禁止分配的地址；<low-address>为起始的 IP 地址，[<high-address>]为结束的 IP 地址，这些地址不会用于动态分配。

举例：192.168.1.1-10 不进行分配

```
Switch (dhcp-config)# ip dhcp excluded-address 192.168.1.1 192.168.1.10
```

7．交换机作为 DHCP 服务器配置案例

某公司网络中定义了一个地址池 neta，地址池网段为 192.168.1.0/24，默认网关为 192.168.1.254，域名为 sgj.com，DNS 为 192.168.1.253，地址租期为 8 天。该地址池中除了 192.168.1.2 至 192.168.1.10 地址外，其余地址均为可分配地址。

具体配置如下：

```
Switch(config)#ip dhcp pool neta  //创建并进入地址池 a
Switch(dhcp-config)#network 192.168.1.0 255.255.255.0 //设置分配的 IP 地址段
Switch(dhcp-config)#default-router 192.168.1.254 //设置默认网关
Switch(dhcp-config)#domain-name sgj.com   //设置域名
Switch(dhcp-config)#dns-server 192.168.1.253  //设置 DNS 的 IP 地址
Switch(dhcp -config)#lease 8   //设置地址租期
```

```
Switch(dhcp-config)#exit
Switch(config)#ip dhcp excluded-address 192.168.1.2 192.168.1.10 //设置排除地址范围
```

注意：交换机做 DHCP 服务器时，能够进行地址分配的前提是交换机必须有相应地址池对应网段的三层接口地址，如交换机上 nata 地址池分配 IP 段为 192.168.1.0/24，则交换机必须有一个 VLAN 对应的三层接口地址为 192.168.1.X/24；可在交换机上建立多个 DHCP 地址池，同时给多个网段分配 IP。

8．DHCP 中继代理工作原理

DHCP 客户端通过广播方式发送 DHCPDISCOVER 发现报文，发现 DHCP 服务器，实现 DHCP 服务功能。在大型网络中，往往划分了多个子网，每个子网是一个广播域，DHCPDISCOVER 发现报文到达子网网关终止，如果 DHCP 客户端及服务器不在同一个广播域内，不能实现 DHCP 服务功能。若要在这种情况下，实现 DHCP 服务功能，需要设置 DHCP 中继代理。

DHCP 中继代理可以在路由器或三层交换机上设置，在 DHCP 客户端及服务器间中转相关报文。DHCP 客户端与代理间仍采用广播方式，DHCP 服务器与代理间采用单播方式，如图 3-13 所示。

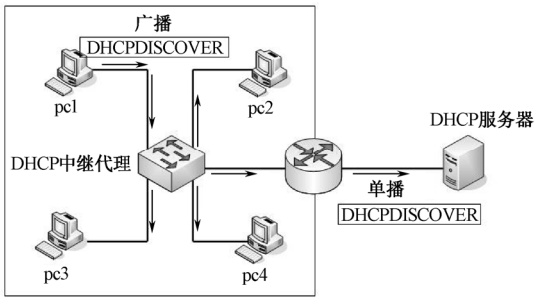


图 3-13　DHCP 中继代理

具体工作过程如下：

（1）发现阶段。客户端使用广播方式发送 DHCPDISCOVER 发现报文，DHCP 中继代理收到后，记录客户端子网地址信息，并以单播方式转发 DHCPDISCOVER 发现报文到达 DHCP 服务器。

（2）提供阶段。当 DHCP 服务器收到 DHCPDISCOVER 发现报文后，根据客户端子网地址信息分配相应子网的地址，并以单播方式发送 DHCPOFFER 提供报文给中继代理。DHCP 中继代理收到 DHCPOFFER 提供报文后，以广播方式转发 DHCPOFFER 提供报文到达客户端子网。

（3）选择阶段。当客户端收到 DHCPOFFER 提供报文后，仍以广播方式发送 DHCPREQUEST 选择报文。DHCP 中继代理收到后，以单播方式发送 DHCPREQUEST 选择报文到达 DHCP 服务器。

（4）确认阶段。当 DHCP 服务器收到 DHCPREQUEST 选择报文后，以单播方式发送 DHCPACK 确认报文给 DHCP 中继代理。DHCP 中继代理以广播方式将 DHCPACK 确认报文转发给客户端，客户端使用 DHCP 服务器分配的 IP 地址及其他网络参数配置网络。

从以上工作过程看出，DHCP 中继代理在 DHCP 客户端及服务器间起到中转服务功能，

从而实现 DHCP 服务器为不同子网提供 DHCP 网络服务。

9．DHCP 中继代理配置

（1）启用 DHCP 服中继代理

命令：service dhcp

no service dhcp

说明：在全局配置模式下，启用 DHCP 服务器和 DHCP 中继代理功能。

举例：开启交换机的 DHCP 服务器或中继代理功能。

```
Switch(config)# service dhcp
```

（2）配置 DHCP 中继转发 DHCP 广播报文

命令：ip forward-protocol udp <port>

no ip forward-protocol udp <port>

说明：在全局配置模式下，配置 DHCP 中继转发 DHCP 广播报文，DHCP 广播报文的 UDP 端口为 67，TFTP 报文的 UDP 端口为 69。

举例：转发 DHCP 广播报文。

```
Switch(config)#ip forward-protocol udp 67
```

（3）指定 DHCP 中继转发 UDP 报文的目标地址

说明：在接口配置或在 VLAN 配置模式下，指定 DHCP 中继转发 UDP 报文的目标地址；DHCP 中继转发的服务器地址是与转发 UDP 的端口相对应的，即 DHCP 中继只转发相应 UDP 协议的报文给相应的服务器，并不是把所有 UDP 报文转发给所有的服务器，缺省配置时 DHCP 中继转发的是 UDP 端口为 67 的 DHCP 报文给 DHCP 服务器。当使用 ip forward-protocol udp <port>命令后，再配置本命令时，本命令所配置的转发地址接收到的是端口号为<port>的 UDP 报文，而非缺省时的 DHCP 报文。

举例：配置 DHCP 中继转发 DHCP 广播报文 UDP 67，且 DHCP 服务器地址为 192.168.1.5。

```
Switch(config)#ip forward-protocol udp bootps
Switch(config)#interface vlan 10
Switch(config-if)#ip helper-address 192.168.1.5
Switch(config-iff)#exit
```

项目实施

任务一　实现酒店内网络互联互通

任务描述

富华大酒店要进行网络的升级改造，经理要求酒店所有办公电脑都连入网络，在娱乐场、会议室等场所加入无线网络，通过调试网络设备实现网络互联互通。

网络拓扑

其网络拓扑结构如图 3-14 所示。

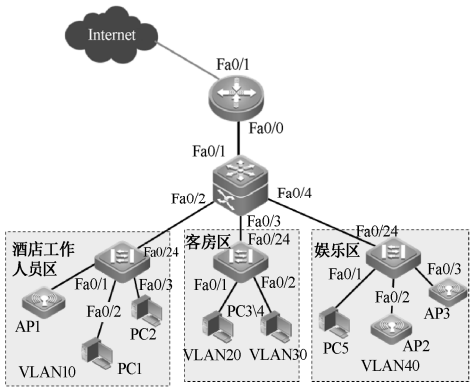


图 3-14　网络拓扑结构图

任务目标

调试交换机和路由器实现全网互通。

设备清单

二层交换机 3 台、三层交换机 1 台、路由器 1 台、双绞线 N 条。

工作过程

步骤一：依照网络拓扑图连接设备，此步略。

步骤二：进行 IP 地址规划

IP 地址规划见表 3-2。

表 3-2　IP 地址表

设　　备	VLAN	IP	接口/说明
酒店工作人员计算机	VLAN10	192.168.10.2/24	Fa0/1～3
客房计算机 A 区	VLAN 20	192.168.20.2/24	Fa0/2
客房计算机 B 区	VLAN 30	192.168.30.2/24	Fa0/3
娱乐及会议区	VLAN 40	192.168.40.2/24	Fa0/1～3
三层交换机 SVI	VLAN 10	192.168.10.1/24	
	VLAN 20	192.168.20.1/24	
	VLAN 30	192.168.30.1/24	
	VLAN 40	192.168.40.1/24	
三层交换机		192.168.50.1/30	Fa0/1
三层交换机	VLAN 1	192.168.255.1/24	管理 IP
路由器	Fa0/0	192.168.50.2/30	Fa0/0
	Fa0/1	200.15.252.2/30	Fa0/1
电信光纤接入 IP		200.15.252.1/30	
接入层交换机 1	VLAN 1	192.168.255.2/24	管理 IP
接入层交换机 2	VLAN 1	192.168.255.3/24	管理 IP
接入层交换机 3	VLAN 1	192.168.255.4/24	管理 IP

步骤三：配置交换机

1．配置接入层交换机

（1）酒店工作人员区 Switch1

```
Switch>enable
Switch#config t
Switch(config)#hostname Switch1
Switch1(config)#vlan 10                    //创建 VLAN
Switch1(config-vlan)#name JDQ
Switch1(config-vlan)#exit
Switch1(config)#interface range fa0/1-3   //进入 fa0/1～3 端口
Switch1(config-if-range)#switchport mode access        //设置端口模式为 access
Switch1(config-if-range)#switchport access vlan 10   //将端口划分给 vlan 10
Switch1(config-if-range)#no shutdown    //激活端口
Switch1(config-if-range)#exit
Switch1(config)#interface fa0/24       //进入 fa0/24 端口
Switch1(config-if)#switchport mode trunk  //设置端口模式为 trunk
Switch1(config-if)#switchport trunk allowed vlan all  //设置允许通过的 VLAN
Switch1(config-if)#no shutdown
Switch1(config-if)#exit
Switch1(config)#interface vlan 1      //进入 vlan 1
Switch1(config-if)#ip address 192.168.255.2 255.255.255.0   //配置 IP 地址
Switch1(config-if)#no shutdown     //激活端口
Switch1(config-if)#exit
Switch1(config)#ip default 192.168.255.1  //设置默认网关
Switch1(config)#exit
Switch1#write
```

（2）酒店工作人员区 Switch2

```
Switch>enable
Switch#config t
Switch(config)#hostname Switch2
Switch2(config)#vlan 20
Switch2(config-vlan)#name KFA
Switch2(config-vlan)#exit
Switch2(config)#vlan 30
Switch2(config-vlan)#name KFB
Switch2(config-vlan)#exit
Switch2(config)#interface fa0/1
Switch2(config-if)#switchport mode access
Switch2(config-if)#switchport access vlan 20
Switch2(config-if)#no shut
Switch2(config-if)#exit
Switch2(config)#interface fa0/2
Switch2(config-if)#switchport mode access
Switch2(config-if)#switchport access vlan 30
```

```
Switch2(config-if)#no shut
Switch2(config-if)#exit
Switch2(config)#interface fa0/24
Switch2(config-if)#switchport mode trunk
Switch2(config-if)#switchport trunk allowed vlan all
Switch2(config-if)#no shut
Switch2(config-if)#exit
Switch2(config)#int vlan 1
Switch2(config-if)#ip address 192.168.255.3 255.255.255.0
Switch2(config-if)#no shut
Switch2(config-if)#exit
Switch2(config)#ip default 192.168.255.1
Switch2(config)#exit
Switch2#write
```

（3）酒店工作人员区 Switch3

```
Switch>enable
Switch#config t
Switch(config)#hostname Switch3
Switch3(config)#vlan 40       //创建 VLAN
Switch3(config-vlan)#name YLQ
Switch3(config-vlan)#exit
Switch3(config)#interface range fa0/1-3  //进入 fa0/1～3 端口
Switch3(config-if-range)#switchport mode access   //设置端口模式为 access
Switch3(config-if-range)#switchport access vlan 40   //将端口划分给 vlan 40
Switch3(config-if-range)#no shutdown        //激活端口
Switch3(config-if-range)#exit
Switch3(config)#interface fa0/24       //进入 fa0/24 端口
Switch3(config-if)#switchport mode trunk  //设置端口模式为 trunk
Switch3(config-if)#switchport trunk allowed vlan all  //设置允许通过的 VLAN
Switch3(config-if)#no shutdown
Switch3(config-if)#exit
Switch3(config)#interface vlan 1     //进入 vlan 1
Switch3(config-if)#ip address 192.168.255.4 255.255.255.0   //配置 IP 地址
Switch3(config-if)#no shutdown    //激活端口
Switch3(config-if)#exit
Switch3(config)#ip default 192.168.255.1     //设置默认网关
Switch3(config)#exit
Switch3#write
```

2．配置三层交换机 Switch4

```
Switch>
Switch>enable
Switch#config t
Switch(config)#hostname Switch4
```

```
Switch4(config)#vlan 10   //创建 VLAN
Switch4(config-vlan)#exit
Switch4(config)#vlan 20
Switch4(config-vlan)#exit
Switch4(config)#vlan 30
Switch4(config-vlan)#exit
Switch4(config)#vlan 40
Switch4(config-vlan)#exit
Switch4(config)#interface vlan 10   //进入 VLAN10
Switch4(config-if)#ip address 192.168.10.1 255.255.255.0  //配置 IP 地址
Switch4(config-if)#no shut
Switch4(config-if)#exit
Switch4(config)#interface vlan 20
Switch4(config-if)#ip address 192.168.20.1 255.255.255.0
Switch4(config-if)#no shut
Switch4(config-if)#exit
Switch4(config)#interface vlan 30
Switch4(config-if)#ip address 192.168.30.1 255.255.255.0
Switch4(config-if)#no shut
Switch4(config-if)#exit
Switch4(config)#interface vlan 40
Switch4(config-if)#ip address 192.168.40.1 255.255.255.0
Switch4(config-if)#no shut
Switch4(config-if)#exit
Switch4(config)#interface range fa0/2-4  //进入 fa0/2-4 端口
Switch4(config-if-range)#switchport mode trunk    //配置端口模式为 trunk
Switch4(config-if-range)#switchport trunk allowed vlan all
Switch4(config-if-range)#no shut
Switch4(config-if-range)#exit
Switch4(config)#ip routing  //启动路由功能
Switch4(config)#int fa0/1
Switch4(config-if)#no switchport  //配置端口为路由端口
Switch4(config-if)#ip address 192.168.50.1 255.255.255.252  //配置 IP 地址
Switch4(config-if)#exit
Switch4(config)#interface vlan 1   //进入 vlan1
Switch4(config-if)#ip address 192.168.255.1 255.255.255.0 //配置 IP 地址
Switch4(config-if)#no shut
Switch4(config-if)#exit
Switch4(config)#ip route 0.0.0.0 0.0.0.0 192.168.50.2  //配置默认路由
Switch4(config)#exit
Switch4#write
```

步骤四：配置路由器

```
Router>enable
Router#config t
```

```
Router(config)#int fa0/0
Router(config-if)#ip address 192.168.50.2 255.255.255.252   //配置 IP 地址
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#int fa0/1
Router(config-if)#ip address 200.15.252.2 255.255.255.252
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#ip route 192.168.0.0 255.255.0.0 192.168.50.1  //配置回指路由
Router(config)#ip route 0.0.0.0 0.0.0.0 200.15.252.1  //配置外出的默认路由
Router(config)#exit
Router#write
```

注意：

1. 如要实现连接因特网还需要进行 NAT 配置，NAT 配置将在项目六中阐述。
2. 无线网络的相关配置已在项目一中阐述，此处不再赘述。

项目测试

第 1 步：在三层交换机上使用 show ip route 命令查看路由表。

```
Switch4#sho ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is 192.168.50.2 to network 0.0.0.0
C    192.168.10.0/24 is directly connected, Vlan10
C    192.168.20.0/24 is directly connected, Vlan20
C    192.168.30.0/24 is directly connected, Vlan30
C    192.168.40.0/24 is directly connected, Vlan40
     192.168.50.0/30 is subnetted, 1 subnets
C       192.168.50.0 is directly connected, FastEthernet0/1
C    192.168.255.0/24 is directly connected, Vlan1
S*   0.0.0.0/0 [1/0] via 192.168.50.2
```

第 2 步：在酒店工作人员计算机 PC1 上使用 ping 命令测试到其他计算机和设备的连通性，见表 3-3。

表 3-3　测试结果

序　号	ping 的地址	结　果	说　明
1	192.168.10.1	通	测试到网关的连通性
2	192.168.20.2	通	测试到客房 A 区电脑的连通性
3	192.168.255.4	通	测试到娱乐区交换机管理 IP 的连通性
4	192.168.50.2	通	测试到路由器 Fa0/0 的连通性

任务二　实现客户自动获取 IP 地址

任务描述

通过对交换机的调试，进行 DHCP 服务器的相关配置，实现计算机自动获取 IP 地址。

网络拓扑

其网络拓扑结构如图 3-15 所示。

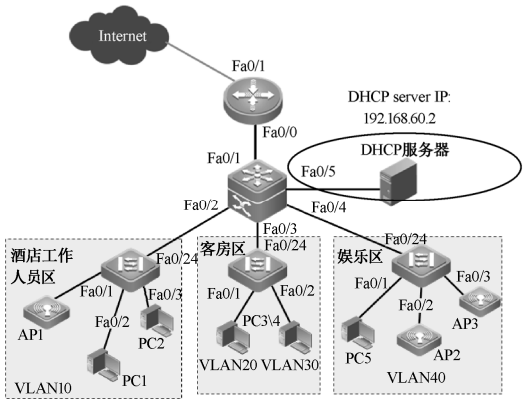


图 3-15　网络拓扑图

任务目标

配置 DHCP 服务器和交换机的 DHCP 中继，实现计算机自动获取 IP 地址。

设备清单

路由器 1 台、交换机 1 台、双绞线 N 条、服务器 1 台。

工作过程

步骤一：连接 DHCP 服务到三层交换机上。

步骤二：配置 DHCP 服务器。

在 DHCP 服务器中，创建 VLAN10、VLAN2、VLAN30 及 VLAN40 的作用域，以 VLAN40 为例，具体操作步骤如下：

（1）单击【开始】，依次选择【管理工具】→【DHCP】，进入到 DHCP 控制台，如图 3-16 所示。

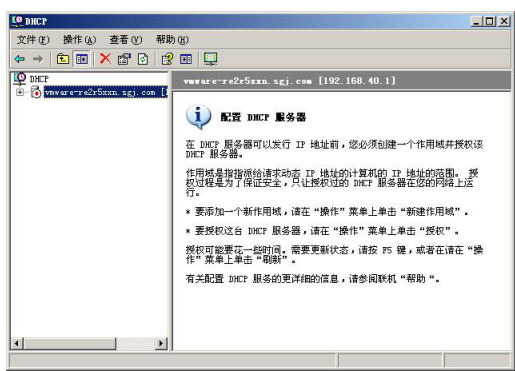


图 3-16　DHCP 控制台

（2）在“DHCP”对话框中单击“操作（A）”，选择“新建作用域（P）”，如图 3-17 所示。

图 3-17　新建作用域

（3）进入配置 DHCP 服务器向导，单击“下一步”按钮，输入作用域名称，如图 3-18 所示。

图 3-18　作用域名

（4）单击“下一步”按钮，在弹出的窗口中输入 IP 地址范围和子网掩码长度。在起始 IP 地址处输入“192.168.40.2”，在结束 IP 地址处输入“192.168.40.253”，在掩码长度处输入“24”，如图 3-19 所示。

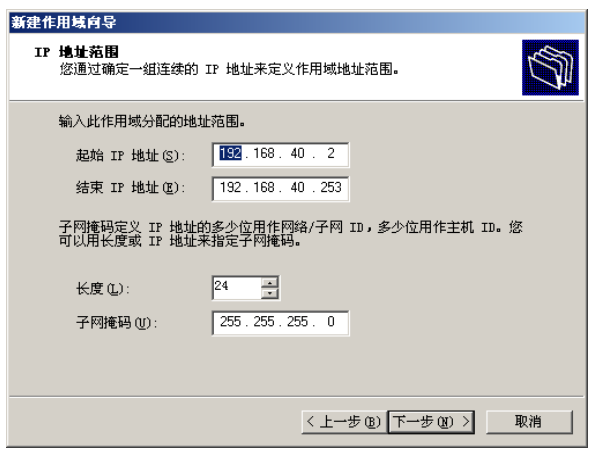


图 3-19　IP 地址范围

（5）单击“下一步”按钮进入“添加排除”向导，这里不需要排除地址，直接单击“下一步”按钮，进入“租约期限”向导，这里不用修改租约期限，直接单击“下一步”按钮，在弹出的窗口中选择“是，我想现在配置这些选项（Y）”，如图 3-20 所示。

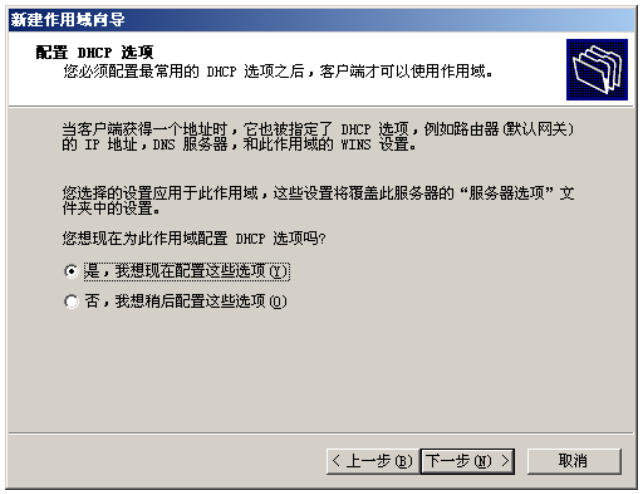


图 3-20　为此作用域配置 DHCP 选项

（6）单击“下一步”按钮，在弹出的窗口中输入路由器（默认网关）的 IP 地址“192.168.40.1”，单击“下一步”按钮。

（7）单击“添加”按钮，然后单击“下一步”，在弹出的窗口中输入 DNS 服务器的相关信息，在 IP 地址处会解析到对应的 IP 地址，或者直接输入 DNS 服务器的 IP 地址，如广东省电信则输入 202.96.128.68，单击“添加”按钮，如图 3-21 所示。

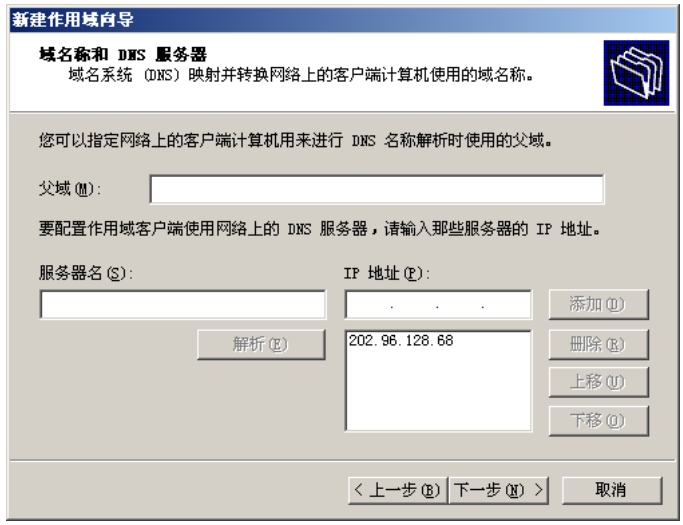


图 3-21　DNS 服务器

（8）单击“下一步”按钮，在弹出的窗口中输入 WINS 服务器信息，默认没有可以不填；直接单击“下一步”按钮，在弹出的窗口中选择“是，我想现在激活此作用域（Y）”。

（9）单击“下一步”按钮，完成 DHCP 作用域的基本配置工作。

步骤三：配置三层交换机

```
Switch4>enable
Switch4#config t
Switch4(config)#interface fa0/5   //进入 Fa0/5 端口
Switch4(config-if)#no switchport  //配置为路由接口
Switch4(config-if)#ip address 192.168.60.1 255.255.255.0  //配置 IP 地址
Switch4(config-if)#no shutdown   //激活端口
Switch4(config-if)#exit
Switch4(config)#service dhcp   //开启交换机 DHCP 服务
Switch4(config)#ip forward-protocol udp 67 //配置 DHCP 报文转发
Switch4(config)#interface vlan 10
Switch4(config-if)#ip helper-address 192.168.60.2  //指定 DHCP 服务器的地址
Switch4(config-if)#exit
Switch4(config)#interface vlan 20
Switch4(config-if)#ip helper-address 192.168.60.2  //指定 DHCP 服务器的地址
Switch4(config-if)#exit
Switch4(config)#interface vlan 30
Switch4(config-if)#ip helper-address 192.168.60.2  //指定 DHCP 服务器的地址
Switch4(config-if)#exit
Switch4(config)#interface vlan 40
Switch4(config-if)#ip helper-address 192.168.60.2  //指定 DHCP 服务器的地址
Switch4(config-if)#exit
Switch4(config)#exit
Switch4#write   //保存配置
```

项目测试

第 1 步：设置本地网卡自动获取 IP，单击“网上邻居”→“属性”→“本地连接”→“属性”→“TCP/IP”，在属性窗口中选择“自动获得 IP 地址”如图 3-22 所示。

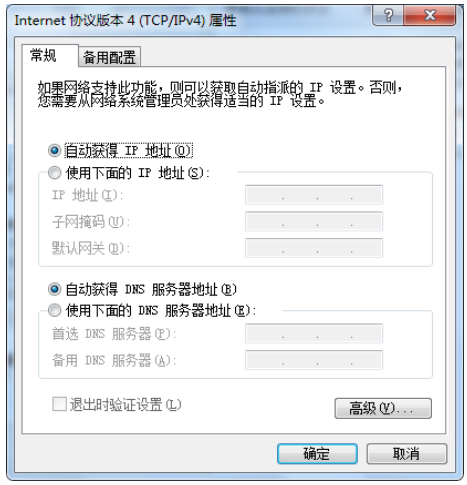


图 3-22　自动获取 IP 地址

第 2 步：在其他计算机可以运行命令 ipconfig/release，进行 IP 释放后再运行 ipconfig/renew

命令重新获取 IP 地址，查看是否自动获取到 IP 地址。

认证测试

一、选择题

1．在交换机配置以下哪个协议可以自动分配 IP 地址（　　）。

A．TCP　　B．DHCP　　C．DN　　D．HTTP

2．局域网内使用 VLAN 所带来的好处是（　　）。

A．可以简化网络管理的配置工作量

B．广播可以得到控制

C．局域网的容量可以扩大

D．可以通过部门等将用户分组而打破物理位置的限制

3．关于 SVI 端口的描述正确的是（　　）。

A．SVI 端口是虚拟的逻辑端口

B．SVI 端口的数量是由管理员设置的

C．SVI 端口可以配置 IP 作为 VLAN 的网关

D．只有三层交换机具有 SVI 端口

4．DHCP 协议使用的传输协议、源端口号、目标端口号是（　　）。

A．TCP　20　21　　B．TCP　67　68

C．UDP　68　67　　D．UDP　67　68

5．DHCP 工作时，客户端与服务器间通信报文有以下 4 种，选择正确工作顺序（　　）。

① 以广播方式发送 DHCPDISCOVER 报文

② 以单播方式发送 DHCPOFFER 报文

③ 以广播方式发送 DHCPREQUEST 报文

④ 以单播方式发送 DHCPACK 报文

A．顺序为 ①→②→③→④　　B．顺序为 ③→②→①→④

C．顺序为 ①→③→②→④　　D．顺序为 ②→①→③→④

6．配置 DHCP 中继命令正确的是（　　）。

A．ip helper-address 192.168.60.2　　B．ip forward-protocol udp 67

C．ip forward-protocol udp 68　　D．ip forward-protocol tcp 67

二、简答题

1．目前有哪些方法能够实现 VLAN 间的通信？

2．比较二层交换机与三层交换机特性，说明它们的异同点？

3．描述配置 SVI 端口使用的命令及步骤？

4．描述 DHCP 的工作过程。

5．说明配置 DHCP 的命令及步骤。

项目四　校园网络的配置与管理

项目背景

华商实验中学占地 200 亩，在校人师生人数 3000 多人。学院有综合办公楼 I 栋，教学楼 2 栋，实验楼 I 栋。学校的信息中心位于综合办公楼 3 层，学校网络拓扑图如图 4-I 所示，近期学校网络中心的交换机 S35A 出现故障，导致 I 号教学楼和综合办公楼无法上网，严重影响了数字化教学和教师办公。学校领导要求网络管理员小李给出学校网络的解决方案，保证网络不出现大范围的网络故障，以提高学校网络的可靠性及可用性。

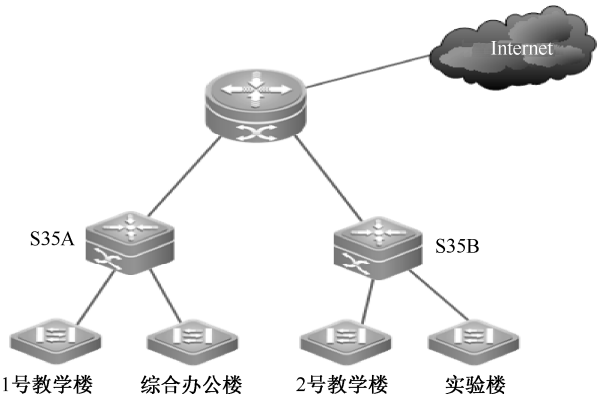


图 4-1　原网络拓扑图

项目分析

小李首先对学校网络设备进行了检查，发现所有接入层交换机都有 I 个多余的光纤接口，S35A 和 S35B 各有 5 个多余的光纤接口。接着小李又分析了学校的网络拓扑结构，发现网络中没有做链路冗余设计，所以很容易出现单点故障。

项目方案

将学校原有网络拓扑结构改为如图 4-2 所示的网络结构，每个接入层交换机都增加一条光纤连接到另一台汇聚交换机上，实现链路冗余连接。两个汇聚交换机间用两条光纤互连，以提高网络的数据交换能力。

图 4-2 的网络结构中的交换机之间形成了网络环路，通过在交换机上配置多实例生成树（MSTP）和虚拟路由器冗余协议（VRRP），解决网络存在的环路问题，并且实现网络的负载均衡，同时可提高网络的性能、可靠性和可用性。

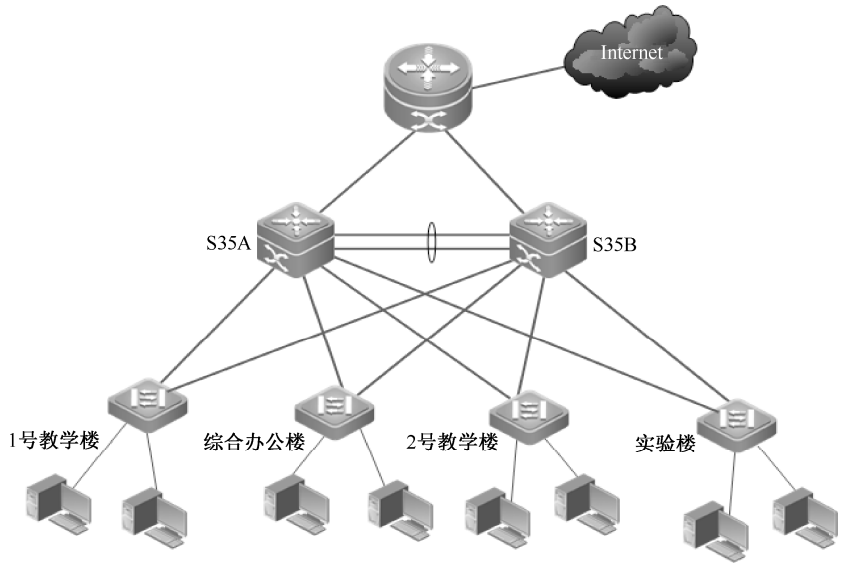


图 4-2　网络拓扑图

知识准备

1．三层网络结构

1）多层设计结构

随着网络技术的迅速发展和网上应用量的增长，分布式的网络服务和交换已经移至用户级，由此形成了一个新的、更适应现代的高速大型网络的分层设计模型。这种分级方法被称为“多层设计”。分层网络设计需要将网络划分成不连续的层，每一层提供特定的功能，与它在整个网络中的角色对应。

园区网通常采用三层结构模型，三层机构模型划分为三个层次，即核心层、汇聚层、接入层，如图 4-3 所示。

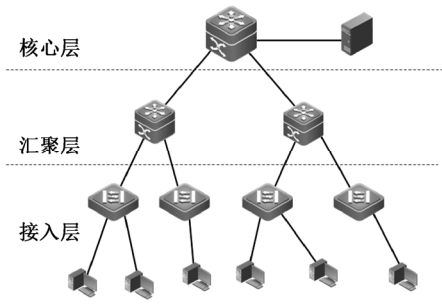


图 4-3　网络三层结构

每个层次完成不同的功能:

（1）核心层 ：核心层作为整个网络系统的核心，其主要功能是高速，可靠地进行数据交换。分层设计的核心层是互联网络的高速骨干，核心层是分发层设备之间互联的关键，因此，其高可用和冗余功能非常重要。核心区域也可以连接到互联网资源，核心层汇聚了来自所有分发层设备的通信，因此，它必须具备快速转发大数据量的能力。

（2）分布层 ：也称汇聚层或分发层，分布层主要进行接入层的数据流量汇聚，并对数据流量进行访问控制。包括访问控制列表、VLAN 路由等。分发层汇聚了从访问层交换机接收到的数据，这些数据都要发送到核心层，然后路由到最终目的地。分发层使用策略和广播域边界控制网络流量，广播域边界是由 VLAN 之间的路由功能实现的，VLAN 是在访问层定义的，它允许你将交换机上的通信分隔成单独的子网，例如，在一所大学的校园网中，可以根据教师、学生和访客来分隔通信。分发层交换机通常是高性能的设备，具有高可用和冗余功能，确保可靠性。

（3）接入层：也称访问层。接入层主要提供最终用户接入网络的途径。主要是进行 VLAN 的划分、与分布层的连接等。访问层与终端设备打交道，如 PC、打印机和 IP 电话，给网络的其余部分提供访问，访问层可以包括路由器、交换机、网桥、集线器和无线访问点。访问层的主要目的是提供一种设备到网络的连接方法，控制哪些设备允许在网络上通信。

2．网络分层设计意义

（1）可伸缩性

分层网络伸缩性非常好，模块化设计允许在网络扩大时直接复制设计元素，因为模块的每一个实例都是一致的，网络扩展更易于规划和实施，例如，如果设计模型是每 10 个访问层交换机配两个接入层交换机，在添加接入层交换机之前，可以继续添加访问层交换机，直到这两个接入层交换机连接的访问层交换机达到 10 个，同样，当接入层交换机达到一定数量后，也应该添加核心层交换机，分担来自接入层交换机的网络流量。

（2）链路冗余

随着网络的增长，可用性变得越来越重要，可以通过分层网络的冗余实现提高其可用性，访问层交换机连接到两个不同的接入层交换机，确保链路冗余，如果某个接入层交换机出现故障，访问层交换机可以转到另一个接入层交换机。此外，接入层交换机也连接到两个或更多核心层交换机，在核心交换机出现故障的情况下，确保链路始终可用。只有访问层不容易做到冗余，通常，每个终端设备，如 PC、打印机和 IP 电话不能连接到多个访问交换机，因为它们往往只有一块网络接口卡，如果访问层交换机出现故障，只有连接到该交换机的终端设备受到影响，网络中的其它设备可以继续正常使用网络。

（3）性能

避免通过低性能，中间交换机传输数据提高通信性能，大多数时候，数据是通过汇聚交换机端口链路从访问层到接入层以近线速发送的，接入层使用它的高性能交换机能力将数据转发给核心层，再路由到最终目的地。因为核心层和接入层以非常快的速度执行它们的操作，不会造成网络带宽竞争。最终，设计良好的分层网络可以实现所有设备之间的近线速数据传输。

（4）安全

在分层网络设计中，安全得到了改善，并且更加易于管理，访问层交换机可以配置多种端口安全选项，控制哪些设备可以连接到网络，在接入层，还可以灵活使用更先进的安全策略来控制，可以应用访问控制策略定义哪些通信协议可以在你的网络上使用，例如，如果想限制某个用户在访问层上使用 HTTP 协议，可以在接入层应用策略阻止 HTTP 通信，基于高层协议约束通信，如 IP 和 HTTP，需要交换机能在那一层处理这些策略，有些访问层交换机也支持 3 层功能，但通常应该由接入层交换机来完成 3 层数据的处理，因为它们处理效率更高。

（5）可管理性

对于分层网络，管理相对来说更简单了，分层设计中的每一层执行特定的功能，因此，如

果需要改变某个访问层交换机的功能，需要同时修改网络中所有访问层交换机的功能，以便保持一致。部署新交换机也很简单，因为交换机的配置可以直接从其它同层设备复制过来，只做少量改动即可。每一层交换机之间的一致性对于快速恢复和简化故障排除都有帮助，在某些特殊情况下，设备之间的配置可能不一致，因此应该确保所有设备的配置都有良好的文档记录，以便于在部署前对比。

（6）可维护性

因为分层网络天生就是模块化的，且具有很好的伸缩性，因此可维护性自然也就很好，对于其它网络拓扑设计，可管理性会随网络的增长变得越来越复杂，同样，在某些网络设计模型中，网络扩容的量是有限制的，不可能无限制地增长，因为它的复杂性会变得几乎不可维护，价格更是高昂。在分层设计模型中，交换机功能是在每一层定义的，正确选择交换机变得更加容易。向某一层添加交换机也并不一定意味着那一层存在瓶颈或其它层存在限制，为了让一个完整的网络拓扑实现性能最大化，所有交换机都需要高性能交换机，因为每个交换机都需要具有执行所有网络功能的能力。在分层模型中，交换机功能在每一层都有所不同，可以在最底层通过使用廉价的访问层交换机来节省成本，在接入层和核心层交换机上花更多的钱，实现高性能的网络。

3．子网划分和子网掩码

（1）子网划分

随着 Internet 的发展，TCP/IP 设计者意识到可用的 IP 地址即将用尽，于是研究人员在 1991 年提供了网络 ID+子网 ID+主机 ID 的 IP 地址划分概念，这种三层结构的子网划分方案允许从一个 IP 地址主机位的最高位开始借用部分位用于网络位来将一个网络划分成几个小的网络，借用的部分表示子网络（即是子网 ID），未借用的部分表示主机（即主机 ID），以便提高 IP 地址的利用率。

（2）子网掩码

引入子网划分技术后，主机路由和路由设备路由如何判断一个给定 IP 地址是否已经进行了子网划分，从而正确地确定 IP 地址中的网络标识呢？因此，将未引入子网划分技术前的地址称为有类别的 IP 地址；将引入子网划分技术后的 IP 地址称为无类别的 IP 地址，并引入子网掩码来描述 IP 地址中关于网络标识和主机号位数的组成情况。

子网掩码使用与 IP 地址相同的由逗号分隔的 4 字节共 32 位数字串的编码格式，二进制形式表现出的特点是由连续的 1 跟随连续的 0 组成，其中连续的 1 对应网络 ID+子网 ID，连续的 0 对应主机 ID。这样，通过子网掩码和 IP 地址按位求反便可以得到网络或子网络的地址。

子网掩码的一个特殊的表示形式：是在 IP 地址后加“/n”n 为网络位和子网位的位数和。这是在配置支持 CIDR 的设备时可以直接使用的形式。

（3）子网划分的方法

根据全 0 和全 1 IP 地址保留的规定，子网划分时至少需要从主机位的高位中借用两位作为子网络位，且 A、B、C 三类网络最多可借用的位数也不同，A 类最多可借 24-2=22 位；B 类最多可借 16-2=14 位；C 类可借 8-2=6 位；具体划分方法如下：

第 1 步：确定子网个数。

2^x-2（x 代表子网位，即二进制为 1 的部分）这里的 x 是指除去默认掩码后的子网位，例如网络地址为 192.168.1.1，掩码为 255.255.255.192，因为是 C 类地址，则掩码为 255.255.255.0。那么 255.255.255.192（x.x.x.11000000）使用了两个 1 来作为子网位。

第 2 步：确定主机数。

2^y-2（y 代表主机位，即二进制为 0 的部分）

第 3 步：有效子网号。

有效子网号=256−10 进制的子网掩码（结果叫做 block size 或 base number）。

第 4 步：每个子网的广播地址。

广播地址=下个子网号−1。

第 5 步：每个子网的有效主机地址。

忽略子网内全为 0 和全为 1 的地址剩下的就是有效主机地址，最后有效 1 个主机地址=下个子网号−2（即广播地址−1）

（4）子网划分的案例

案例 1：有一个 C 类网络地址 192.168.10.0 子网掩码为 255.255.255.192（/26）则：

1．子网数=$2^2-2=2$

2．主机数=$2^6-2=62$

3．有效子网：block size=256−192=64；所以第一个子网为 192.168.10.64，第二个为 192.168.10.128

4．广播地址：下个子网−1。所以 2 个子网的广播地址分别是 192.168.10.127 和 192.168.10.191

5．有效主机范围是：第一个子网的主机地址是 192.168.10.65 到 192.168.10.126；第二个是 192.168.10.129 到 192.168.10.190

具体 IP 分配表如表 4-1 所示。

表 4-1 C 类地址 192.168.10.0/26 划分子网

子 网	子 网 号	子 网 地 址	有效主机地址范围	广 播 地 址	子 网 掩 码
1	00	192.168.10.0	192.168.10.1.62	192.168.10.63	255.255.255.192
2	01	192.168.10.64	192.168.10.65.126	192.168.10.127	255.255.255.192
3	10	192.168.10.128	192.168.10.129.190	192.168.10.191	255.255.255.192
4	11	192.168.10.192	192.168.10.193.254	192.168.10.255	255.255.255.192

在表 4-3 中虽然子网个数共有 4 个，但根据全 0 和全 1IP 地址保留的规定，所以有效子网是 01 和 10 这两个子网，第一个子网为 192.168.10.64，第二个为 192.168.10.128。

案例 2：有一个 C 类网络地址为 192.168.10.0；子网掩码为 255.255.255.128(/25)则：

（1）子网数=2

（2）主机数=$2^7-2=126$

（3）有效子网：block size=256−128=128； 所以第一个子网为 192.168.10.0；第二个为 192.168.10.128。

（4）广播地址：下个子网−1；所以 2 个子网的广播地址分别是 192.168.10.127 和 192.168.10.255。

（5）有效主机范围是：第一个子网的主机地址是 192.168.10.1 到 192.168.10.126;第二个是 192.168.10.129 到 192.168.10.254。

具体如表 4-2 所示。

表 4-2　C 类地址 192.168.10.0/25 划分子网

子　网	子 网 号	子 网 地 址	有效主机地址范围	广 播 地 址	子 网 掩 码
1	00	192.168.10.0	192.168.10.0～.126	192.168.10.127	255.255.255.128
2	01	192.168.10.128	192.168.10.129～.254	192.168.10.255	255.255.255.128

只向主机位借 1 位的特殊情况是 RFC 文档所规定不允许的，但在路由器的全局配置模式下输入“ip subnet –zero”命令来告诉你的路由器打破规则并使用一个 1 位的子网掩码，就可以让每个子网拥有 126 台主机了。

4．路由汇总

路由汇总也叫路由汇聚，是把一组路由汇聚为一个单个的路由广播。路由汇聚的最终结果和最明显的好处是缩小网络上的路由表的尺寸。这样将减少与每一个路由的延迟，由于减少了路由项数量，查询路由表的平均时间将加快。由于路由项广播的数量减少，路由协议的开销也将显著减少。随着整个网络（以及子网的数量）的扩大，路由汇聚将变得更加重要，如图 4-4 所示。

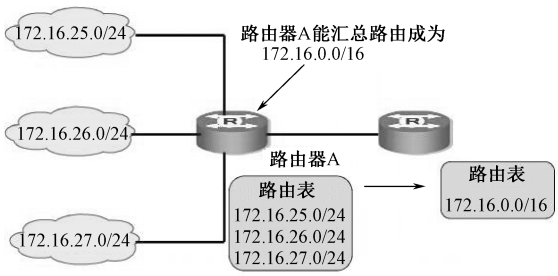


图 4-4　路由汇总

汇总的方法通常是在字节内进行汇总，找出 IP 地址二进制数中共同的比特位就是路由汇总的地址，如图 4-5 所示。

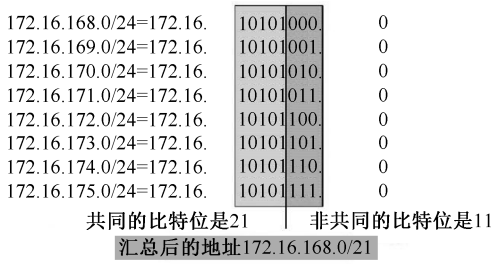


图 4-5　汇总方法

5．校园网 IP 地址规划

（1）校园网 IP 地址分类

校园网 IP 地址资源现状是大部分学校获得的公共 IP 地址数量较少，采用 NAT（网络地址转换）的方式接入教育网及互联网，所以私有 IP 地址在校园网内应用普遍。包含以下几种：

- 10.0.0.0-10.255.255.255　　A 类私有地址
- 172.16.0.0-172.31.255.255　　B 类私有地址
- 192.168.0.0-192.168.255.255　C 类私有地址

对于小型校园网，如单核心二层结构的中小学校园网，上网用户少、设备数量少的建议采用地址空间小的 192.168.0.0/16 网段，而中型校园网，如三层结构的校园网上网人数多、设备数量多、网络后期建议采用地址空间中的 172.16.0.0/12 网段，超大型校园网的建议使用地址空间最大的 10.0.0.0/8 网段。

（2）校园网 IP 地址设计原则

校园网 IP 地址设计原则是可扩展、可汇总、易管理、易维护的原则。

可扩展性与可汇总性在校园网 IP 地址中尤其重要，可扩展性可以将一个 IP 地址段分为数个子网用于校园网的各个区域或部门使用；而可汇总性指 IP 在路由汇总时能缩小网络上的路由表的尺寸，这样将减少与每一个路由的延迟，查询路由表的平均时间将加快。由于路由项广播的数量减少，路由协议的开销也将显著减少，网络变得更快速有效。可扩展性与可汇总性 IP 地址设计如图 4-6 所示。

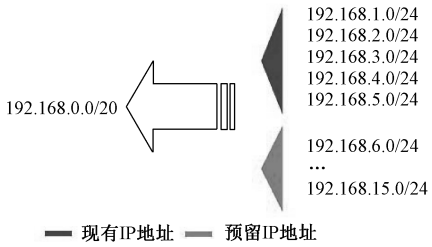


图 4-6　可扩展与可汇总的 IP 地址设计

为使校园网更具有可管理性与可维护性，在校园 IP 地址设计时要考虑到可管理性与可维护性，除了给用户 IP（分配给每个最终用户 PC 或服务器使用）外，我们还应该给出设备管理 IP 与设备互联 IP 用于网络管理员远程管理和三层设备之间互联。易管理的 IP 地址设计如图 4-7 所示。

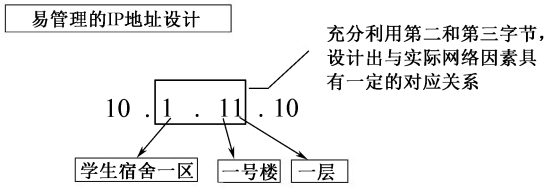


图 4-7　易管理的 IP 地址设计

6．端口聚合

1）端口聚合技术

端口聚合（Aggregate-port）也叫链路聚合，可以将多物理连接当作一个单一的逻辑连接来处理，它允许两个交换机之间通过多个端口并行连接同时传输数据以提供更高的带宽、更大的吞吐量和可恢复性的技术。增大链路带宽解决了交换网络中因带宽引起的网络瓶颈问题。多条物理链路之间能够相互冗余备份，其中任意一条链路断开，不会影响其他链路的正常转发数据。

端口聚合是遵循 IEEE802.3ad 协议的标准，一般来说，两个普通交换机连接的最大带宽取决于媒介的连接速度，如 100BAST-TX 双绞线为 200M，而使用端口聚合技术可以将 4 个 200M

的端口捆绑后成为一个高达 800M 的连接，如图 4-8 所示。

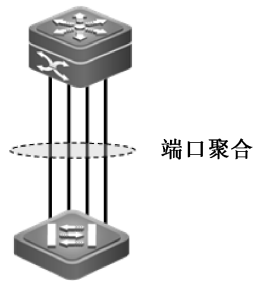


图 4-8　端口聚合

这一技术的优点是以较低的成本通过捆绑多端口提高带宽，而其增加的开销只是连接用的普通五类网线和多占用的端口，它可以有效地提高子网的上行速度，从而消除网络访问中的瓶颈。通常端口聚合技术是应用于交换机与交换机间的技术，通常是通信主干道，而干道 Trunk 技术具有自动带宽平衡，即容错功能：即使 Trunk 只有一个连接存在时，仍然会工作，这无形中增加了系统的可靠性。

端口聚合的优点：

（1）带宽增加，带宽相当于组成组的端口的带宽总和。

（2）增加冗余，只要组内不是所有的端口都 down 掉，两个交换机之间仍然可以继续通信。

（3）负载均衡，可以在组内的端口上配置，使流量可以在这些端口上自动进行负载均衡。

2）端口聚合配置

以图 4-9 为例，在两台交换机之间连接了两条网线，通过相关端口聚合的配置，来提高链路带宽，提供冗余链路。

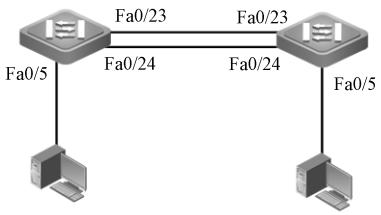


图 4-9　端口聚合配置

以左边交换机为例，做以下配置。

```
SwitchA(config)#interface aggregateport 1  //进入聚合端口 1
SwitchA(config-if)#Switchport mode trunk    //设置端口的工作模式是 Trunk
SwitchA(config-if)# Exit
SwitchA(config)#Interface range fastethernet 0/23-24   //进入端口
SwitchA(config-if)#Port-group 1      //配置为端口组 1
SwitchA(config-if)#end
SwitchA#Show aggregateport 1 summary //验证接口 fastethernet 0/23 和 0/24 属于 AG1
```

在配置交换机的端口聚合时，应注意只有同类型端口才能聚合为一个 AG 端口，所有物理端口必须属于同一个 VLAN，有的交换机上最多支持 8 个物理端口聚合为一个 AG 和最多支持 6 组聚合端口。

7．生成树协议

1）生成树协议概述

交换机之间具有冗余链路本来是一件很好的事情，但是它有可能引起的问题比它能够解决的问题还要多。如果真的准备两条以上的链路，就必然形成了一个环路，交换机并不知道如何处理环路，只是周而复始地转发帧，形成一个“死循环”，这个死循环会造成整个网络处于阻塞状态，导致网络瘫痪，如图 4-10 所示。

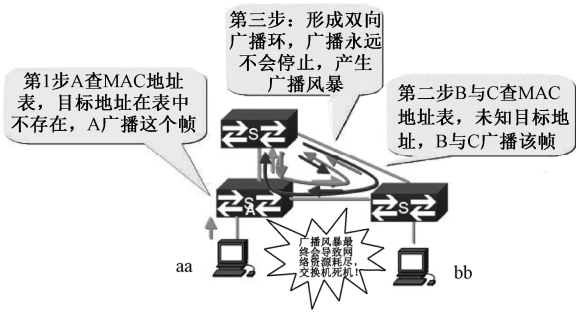


图 4-10　广播风暴导致交换机死机

冗余链路是提高网络的可用性，减少网络故障时间的重要措施，但交换机的基本工作原理导致了这样的设计可能会在交换网络中产生广播风暴等问题。生成树协议是在既能保证冗余链路提供链路备份，又能避免环路、广播风暴等问题而产生的技术。

生成树协议的主要功能就是为了解决网络中由于备份连接所产生的环路问题。当网络中有环路时，生成树协议通过生成树算法（Spanning Tree Algorithm）生成一个没有环路的网络，当主要链路出现故障时，能够自动切换到备份链路，保证网络的正常通信。具体的实现方法是：生成树协议通过交换机运行生成树算法，先使冗余端口置于“阻塞状态”，这样使网络中的计算机在通信时只有一个链路有效；而当这个链路出现故障时，生成树协议将会重新计算出网络的最优链路，将原处于“阻塞状态”的部分重新打开，从而确保网络连接的稳定性和可靠性，如图 4-11 所示。

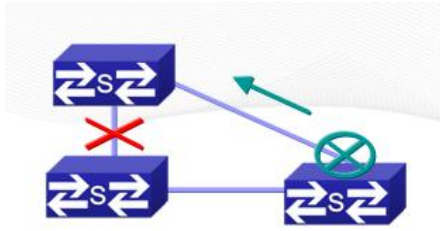


图 4-11　冗余端口置于“阻塞状态”

在生成树协议发展过程中，不断克服以前的缺陷，并不断开发新的功能。按照功能的改进情况，我们把生成树的发展过程划分为三代。

第一代生成树协议：STP/RSTP

第二代生成树协议：PVST/PVST+

第三代生成树协议：MISTP/MSTP

其中最常用的协议是 STP（生成树协议）、RSTP（快速生成树协议）和 MSTP（多实例生成树协议）。

2）生成树配置命令

（1）开启生成树协议

命令：spanning-tree

no spanning-tree

说明：在交换机的全局配置模式和端口配置模式下分别启动 MSTP 协议的命令；本命令的 no 操作为关闭 MSTP 协议。系统缺省不运行 MSTP 协议。但如果在全局配置模式下启动了 MSTP 协议，所有的端口缺省都打开 MSTP 协议。

举例：在全局模式打开 MSTP，并且在端口 fa0/2 模式关闭 MSTP。

```
Switch(config)#spanning-tree
Switch(config)#interface fa0/2
Switch(config-if-ethernet0/0/2)#no spanning-tree
```

（2）设置 Spanning Tree 的模式

命令：spanning-tree mode { stp/rstp }

no spanning-tree mode

说明：设置交换机运行 Spanning Tree 的模式；本命令的 no 操作为恢复交换机缺省的模式。mstp 为设置交换机运行 IEEE802.1s 的 MSTP 模式；stp 为设置交换机运行 IEEE802.1D STP 模式。

举例：设置交换机运行 STP 模式。

```
Switch(config)#spanning-tree mode stp
```

（3）显示交换机 Spanning Tree 信息

命令：show spanning-tree

说明：特权模式下，通过 show spanning-tree 命令可以查看该网桥及各实例的 MSTP 信息，域配置信息以及端口的 MSTP 信息等。

举例：特权模式下显示生成树信息。

```
SW1#sh spanning-tree
```

3）多生成树协议

MSTP 协议是一个多生成树（Multi Spanning Tree，MST）协议，相对 RSTP 来说，主要是引入了实例和域的概念。域的概念是为了将网络中具有不同配置的网络段进行分割开，在网络段内部实行统一的配置，可以在域内进行独立的生成树构造。而域之间则使用一个单一生成树将所有的域连接起来（该生成树被称为 CST，公共生成树），确保全链接和无环。在域的内部可以构造多个生成树实例，同时可以将不同的 VLAN 映射到不同的生成树实例上。在每个域的内部都有一个实例 ID 为 0 的实例，该实例与 CST 共同组成了 CIST（公共内部生成树）。该生成树将整个网络中的域和域内部的桥设备和网段连成一个全链接无环的树。

（1）MSTP 协议的基本概念

MST 域：是由交换网络中的多台设备以及它们之间的网段所构成。这些设备具有下列特点：都启动了 MSTP；具有相同的域名；具有相同的 VLAN 到生成树实例映射配置；具有相同的 MSTP 修订级别配置；这些设备之间在物理上有链路连通。

MST Configuration Identifier：用来标示一个 bridge 的 MST 配置内容，以确定桥与桥之间是否能够在同一个域内。内容包括 Configuration Identifier Format Selector，Configuration Name，Revision Level，Configuration Digest。

CIST Root Identifier：CIST 根桥的桥 ID。

CIST External Root Port Cost：CIST 外部根路径开销，是指一个桥所在的域到 CIST 根桥所在的域之间的路径开销，在一个域内所有桥的 CIST External Root Port Cost 都是一样的，在计算的时候 CIST 指计算域的根桥的根端口所在 LAN 的路径开销。

Regional Root Identifier：域的根桥的桥 ID，域的根桥并不是在域内的所有桥中 ID 最小的一个，而是域内到 CIST 根桥的根路径开销最低的桥。

Internal Root Port Cost：内部路径开销是指将域看作一个独立的局域网，域内的桥设备到域的根桥的根路径开销。

Master Port：Master Port 是指一个域中根桥的根端口。该域通过该端口到达根桥的路径最小。VLAN 映射表：VLAN 映射表是指将 VLAN 映射到某个具体的 MSTI，在同一个域内所有

桥设备的 VLAN 映射表必须保持一致，默认情况所有 VLAN 映射到实例 0。

CST：Common Spanning Tree，用于联通不同域或非 MSTP 桥设备的生成树。

（2）端口角色

■ 根端口/主端口（Root Port/Master Port），交换机上到总根具有最短路径的端口称为根端口（Root Port），如果该交换机是主交换机，则相应的根端口为该域的主端口，根端口负责向总根转发数据流量。

■ 指定端口（Designated Port），局域网上到总根具有最短路径的端口称为指定端口，指定端口负责为所在的局域网转发数据流量。

■ 选择端口（Alternate Port），局域网上处于备份地位的端口称为选择端口，选择端口不转发数据流量。

■ 备份端口（Backup Port），交换机上连接到自己且端口状态为丢弃的端口称为备份端口。

（3）MSTP 特点

■ MSTP 设置 VLAN 映射表，即 VLAN 和生成树实例的对应关系，把 VLAN 和生成树联系起来，通过增加实例（多个 VLAN 整合到一个集合中）这个概念，将多个 VLAN 捆绑到一个实例中，以节省开销和资源占用率。

■ MSTP 把一个交换网络划分为多个域，每个域内形成多棵生成树，生成树之间彼此独立。

■ MSTP 将环路剪成一个无环的树形网络，避免报文在环路中增加和无限循环，同时还提供了数据转发的多个冗余路径，在数据库转发过程中实现 VLAN 数据的负载分担。

（4）配置 MSTP 协议步骤

步骤一：启用生成树协议并制定类型。

```
SW(config)#spanning-tree              //开启生成树
SW(config)#spanning-tree mode mstp  //配置生成树类型
```

步骤二：创建生成树协议实例并指定版本。

```
SW(config)#spanning-tree mst configuration
SW(config-mst)#instance 1 VLAN 10,30   //将 vlan10、30 关联到实例 1 中，每个实例都会生成一个独立的生成树
SW(config-mst)#revision 1              //配置多生成树的版本号
SW(config-mst)#instance 2 vlan 20,40   //将 vlan20、40 关联到实例 2 中
SW (config-mst)#revision 1
SW (config-mst)#exit
```

步骤三：制定优先级。

```
SW (config)#spanning-tree mst 1 priority 4096  //实例 1 在 SW 的优先级为 4096
SW (config)#spanning-tree mst 2 priority 8192  //实例 2 在 SW 的优先级为 8192
```

步骤四：通常两台交换机同时配置，主要区别在于实例 1 和实例 2 在不同的交换机上配置优先级不同。

8．VRRP 协议

VRRP 协议（Virtual Router Redundancy Protocol，虚拟路由器冗余协议）与 HSRP 类似，能够提高网络的稳定性和可靠性，其由 IETF 标准 RFC2338 定义。由于 VRRP 与 HSRP 原理类似，只是术语和功能上有细微的差别。

1）VRRP 的工作原理

如图 4-12 所示，VRRP 协议将 LAN 网段上的两台或者多台路由器作为一台“虚拟”路由器使用，通过同一个虚拟 IP 地址和虚拟 MAC 地址而对外提供服务。如果其中一台出现故障，另一台就能接替它，继续完成路由功能。

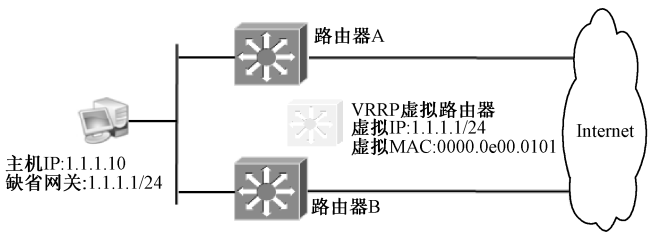


图 4-12　VRRP 创建了一个有自己 MAC 地址和 IP 地址的虚拟路由器

VRRP 协议组中包括一台主路由器、备份路由器和一台虚拟路由器。VRRP 协议中活跃路由器称为主路由器，其转发发送到虚拟路由器的数据包。而其他 VRRP 组中非主路由器的路由器都处于备份状态。虚拟路由器是向最终用户代表一台可以连续工作的路由器。

VRRP 与 HSRP 相同，根据优先级大小选择主路由器，同一个 VRRP 组中优先级最大的路由器称为主路由器，状态为 Master。组中其他路由器都处于备份状态，并检测主路由器的状态。主路由器每隔一段时间会发送一个 VRRP 通告，通告其工作正常。如果 VRRP 组中的备份路由器长时间没有收到主路由器的通告，就将自己改为 Master 状态。VRRP 组内可能有多台备份路由器同时认为自己是主路由器，这时每台主路由器都会比较收到的 VRRP 通告中的优先级与本地优先级的大小。如果本地优先级小于 VRRP 通告的优先级，则自身路由器状态为备份状态，否则为 Master 状态不变。最终一个 VRRP 组中优先级最大的路由器成为新的主路由器。

2）虚拟 MAC 地址

VRRP 组中虚拟路由器的 MAC 地址格式为 0000.5e00.01xx，其中 xx 为 VRRP 组号。

例如：VRRP 组 47，则虚拟路由器的 MAC 地址是 0000.5e00.012f。

3）VRRP 通告

VRRP 协议中只定义了一种报文即 VRRP 通告，其使用 IP 协议号为 112，目的地址为组播地址 224.0.0.18。

4）VRRP 的状态

VRRP 协议共定义了三种状态：Master（主状态）、Backup（备份状态）、Initialize（初始状态）。

（1）初始状态：所有路由器都从初始状态开始，即进程启动后进入此状态。

（2）备份状态：接收主路由器发送的 VRRP 组播通告，由此判断主路由器的状态；丢弃发送到虚拟路由器的 MAC 地址和 IP 地址的数据包；不响应对虚拟 IP 地址的 ARP 请求。

（3）主状态：定期发送 VRRP 组播通告；响应对虚拟 IP 地址的 ARP 请求，并且发送免费 ARP 报文使网络内主机知道虚拟 IP 地址和虚拟 MAC 地址的对应关系；转发目的地址是虚拟 MAC 地址的 IP 数据包。

VRRP 三种状态间的转换关系如图 4-13 所示。

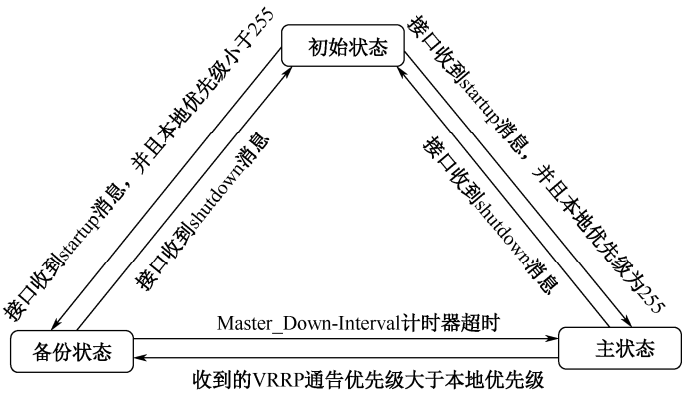


图 4-13　VRRP 三种状态之间的转换关系

在初始状态如果接收到 startup 消息，并且优先级为 255（优先级范围 0～255）时，则路由器状态转为主状态；如果优先级小于 255 时，则路由器状态转为备份状态。

在备份状态如果接口收到 shutdown 消息，则路由器状态转为初始状态；如果 Master_Down_Interval 时间超时，则路由器转为主状态。

在主状态如果接口收到 shutdown 消息，则路由器状态转为初始状态；如果接收到的 VRRP 组播通告中的优先级大于本地优先级，则路由器状态转为备份状态。

1．Master_Down_Interval 相当于 HSRP 中的保持时间，即备份路由器一段时间没有收到主路由器的 VRRP 通告，则认为主路由器异常，自身成为主路由器。

2．VRRP 优先级与 HSRP 优先级相同，范围是 0～255，可以配置的范围是 1～254，默认为 100。如果 VRRP 配置的虚拟 IP 地址和路由器的实际物理接口地址相同时，这个 VRRP 路由器称为 IP 地址拥有者，这时此路由器的 VRRP 优先级为 255。

5）VRRP 计时器

VRRP 通告的发送时间默认为 1s，而 Master_Down_Interval 时间是 3 倍的主路由器 VRRP 通告发送时间再加上一个偏移时间，具体的计算公式详见 RFC2338。

6）VRRP 认证

VRRP 协议提供了三种认证方式（无认证、简单字认证和 MD5 认证）可以根据不同的网络环境使用不同的认证方式。在一个安全的网络中可以使用无认证，在一个十分不安全的网络中可以使用 MD5 认证。

7）VRRP 的配置

（1）将路由器配置为 VRRP 组成员

命令：Switch(config-if)#vrrp *group-number* ip *virtual-ip-address*

说明：将路由器或三层交换机配置为 VRRP 组的成员，并指定虚拟 IP 地址，group-number：表示该端口所属的 VRRP 组。可配置范围是 1～255。*virtual-ip-address*：表示虚拟 VRRP 路由

器的 IP 地址，即网段的网关地址。如果虚拟 IP 地址和接口的物理 IP 地址相同，则此 VRRP 组中本地路由器的优先级为 255。

（2）配置 VRRP 优先级，优先级数值高的将成为主路由器

命令：Switch(config-if)#vrrp group-number priority priority-value

说明：用户可以指定端口在组内的优先级。这样，在出现故障时，用户可以灵活地指定端口顺序。priority-value 范围是 0～255，可配置范围是 1～254，默认值是 100。需要注意如果路由器是 IP 地址拥有者则优先级为 255，无法配置优先级。

（3）配置占先权

命令：Switch(config-if)#vrrp group-number preempt

说明：可以使用 no vrrp *group-number* preempt 命令开启 VRRP 占先权，占先权的含义与 HSRP 相同，但是 VRRP 协议中占先权默认是开启的。

（4）配置 VRRP 定时器

命令：Switch(config-if)#vrrp 1 timers advertise [msec] interval

说明：其中，使用 msec 参数配置的时间间隔为毫秒，范围 50～999；不使用 msec 参数配置的时间间隔为秒，范围是 1～255。命令 vrrp *group-number* timers learn 为从主路由器那里获悉 VRRP 通告时间间隔，由此计算 Master_Down_Interval 的时间。

（5）配置 VRRP 认证

VRRP 配置明文认证的命令为：

```
Switch(config-if)#vrrp 1 authentication word
```

VRRP 配置 MD5 认证的命令为：

```
Switch(config-if)#vrrp 1 authentication md5 key- string word
```

（6）配置 VRRP 端口跟踪

VRRP 配置端口跟踪的方式与 HSRP 稍有不同。VRRP 配置端口跟踪时，首先，需要定义跟踪的端口命令如下：

```
Switch(config-if)#track number interface type mod/mun line-protocol
```

说明：*number* 为编号，范围 1～500；line-protocol 表示接口链路层状态。

然后，在接口模式下配置 VRRP 端口跟踪，命令为：

```
Switch(config-if)#vrrp group-number track number decrement interface-priority
```

说明：group-number：采用跟踪功能的端口的 VRRP 组号；number：跟踪由 track number 所定义的端口；interface-priority：当端口失效时路由器的热备份优先级将降低的数值；当端口变为可用时，路由器的优先级将加上该数值。

要关闭端口跟踪功能时，可以使用 no standby group-number track 命令。

需要注意如果路由器是 IP 地址拥有者则优先级为 255，不能配置端口跟踪。

（7）查看 VRRP 路由器状态

要显示 VRRP 路由器的状态，在特权模式下输入如下命令：

```
Switch#show vrrp [interface type mod/mun] [group group-number] [brief]
```

说明：interface type mod/mun:要显示的端口类型和序号；group group-number:要显示的具体 VRRP 组；brief：显示摘要信息，每个备份组总结显示一行输出。

如果没有指定这些任选端口参数，那么，show vrrp 命令可以显示所有端口的 VRRP 信息。

案例：使用 show vrrp brief 命令显示所有端口的 VRRP 信息。

```
SW1#show vrrp brief
Interface      Grp Pri Time  Own Pre State   Master addr     Group addr
Vl2            2   150 3414      Y  Master  192.168.2.1     192.168.2.254
```

此输出表明，VLAN2 端口参与了 VRRP 2 组，优先级为 150，启用了占先权，不是 IP 地址拥有者，这个路由器处于 Master 状态，组中主路由器的 IP 地址为 192.168.2.1，VRRP 组的虚拟 IP 地址是 192.168.2.254。

使用 show vrrp 命令可以查看 VRRP 的详细信息，如下所示：

```
SW1#show vrrp
Vlan2 - Group 2                                          //VRRP 组号
State is Master                                          //状态为 Master
Virtual IP address is 192.168.2.254                      //VRRP 组的虚拟 IP 地址
Virtual MAC address is 0000.5e00.0102                    //VRRP 组的虚拟 MAC 地址
Advertisement interval is 1.000 sec                      //VRRP 通告发送时间间隔
Preemption enabled                                       //占先权为启动状态
Priority is 150                                          //优先级为 150
Track object 1 state Up decrement 100                    //端口跟踪，降低优先级 100
Master Router is 192.168.2.1 (local), priority is 150 //主路由器的信息
Master Advertisement interval is 1.000 sec               //主路由器的 VRRP 通告时间
                                                           间隔
Master Down interval is 3.414 sec                        //主路由器的 Down interval
                                                           时间
Vlan3 - Group 3
State is Backup
Virtual IP address is 192.168.3.254
Virtual MAC address is 0000.5e00.0103
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 100
Master Router is 192.168.3.2,  priority is 150
Master Advertisement interval is 1.000 sec
Master Down interval is 3.609 sec (expires in 3.217 sec) Learning  //学习到的
主路由器 Down interval 时间
```

项目实施

任务一　实现校园网内部通信

任务描述

网络管理员小李已经在学校原有网络的接入层交换机上都增加了一条光纤连接到另一台汇聚

交换机上，实现链路冗余连接，并在两个汇聚交换间用两条光纤进行了互连，连接后的学校网络拓扑结构如图 4-15 所示。现在小李需要在交换机上配置多实例生成树（MSTP）和虚拟路由器冗余协议（VRRP），以解决网络存在的环路问题，并且实现网络的负载均衡，同时可提高网络的性能、可靠性和可用性。假如你是小李，请你帮他完成该任务。

网络拓扑

其网络拓扑结构如图 4-14 所示。

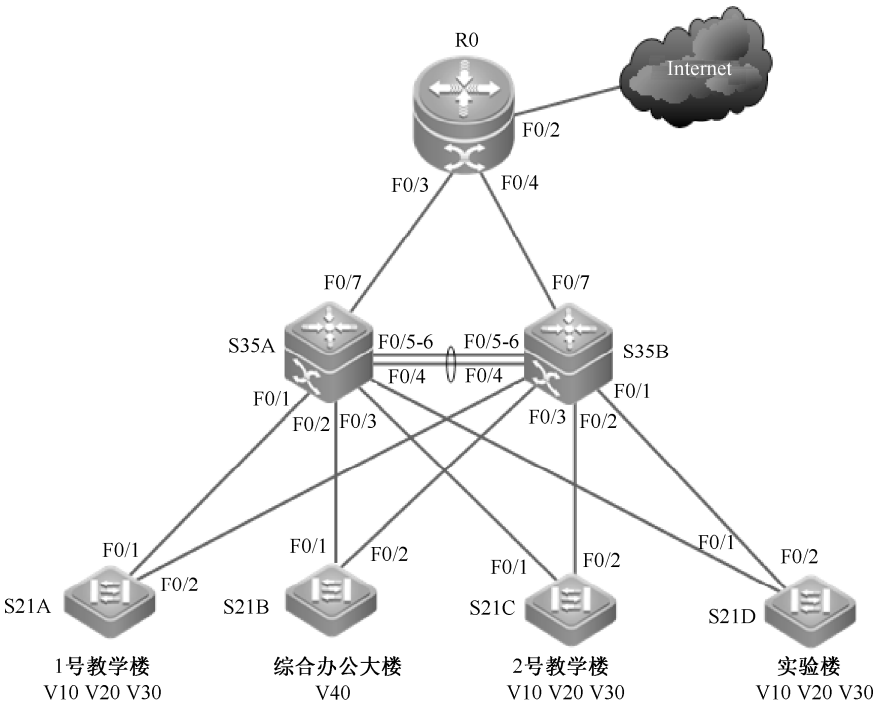


图 4-14　校园网络拓扑结构图

任务目标

1．解决网络环路问题，实现网络的负载均衡；

2．提高网络的性能、可靠性和可用性。

设备清单

路由器 1 台，三层交换机 2 台，接入层交换机 4 台，双绞线 N 条。

工作过程

步骤一：制作双绞线，并连接设备。

略（详细见项目一的制作过程）

步骤二：进行 VLAN 及 IP 地址规划（见表 4-3）

表 4-3 网络设备 IP 地址表

VLAN 号	网 络 地 址	备 注
Vlan10	192.168.10.0/24	1 年级教师办公室
Vlan20	192.168.20.0/24	2 年级教师办公室
Vlan30	192.168.30.0/24	3 年级教师办公室
Vlan40	192.168.40.0/24	综合办公楼办公室
设 备 名 称	接 口	IP 地址
R0	F0/2	182.100.1.2/28
	F0/3	172.16.1.2/24
	F0/4	172.16.2.2/24
S35A	F0/7	172.16.1.1/24
	Vlan10	192.168.10.2/24
	Vlan20	192.168.20.2/24
	Vlan30	192.168.30.2/24
	Vlan40	192.168.40.2/24
S35B	F0/7	172.16.2.1/24
	Vlan10	192.168.10.3/24
	Vlan20	192.168.20.3/24
	Vlan30	192.168.30.3/24
	Vlan40	192.168.40.3/24

步骤三：配置交换机。

第 1 步：配置接入层交换机 S21A。

（1）开启生成树

```
S21A (config)#spanning-tree                 //开启生成树
S21A (config)#spanning-tree mode mstp       //配置生成树模式为 MSTP
```

（2）创建 VLAN

```
S21A(config)#vlan 10    //创建 Vlan 10
S21A(config)#vlan 20    //创建 Vlan 20
S21A(config)#vlan 30    //创建 Vlan 30
```

（3）划分 VLAN 端口

```
S21A(config)#interface range fastethernet 0/3-7
S21A(config-if)#switchport access vlan 10      //分配端口 F0/3-7 给 Vlan 10
S21A(config)#interface range fastethernet 0/8-12
S21A(config-if)#switchport access vlan 20      //分配端口 F0/8-12 给 Vlan 20
S21A(config)#interface range range fastethernet 0/13-17
S21A(config-if)#switchport access vlan 30      //分配端口 F0/13-17 给 Vlan 30
```

（4）配置 Trunk

```
S21A(config)#interface fastethernet 0/1
```

```
S21A(config-if)#switchport mode trunk      //定义 F0/1 为 trunk 端口
S21A(config)#interface fastethernet 0/2
S21A(config-if)#switchport mode trunk      //定义 F0/2 为 trunk 端口
```

（5）配置实例关联 VLAN

```
S21A(config)#spanning-tree mst configuration    //进入 MSTP 配置模式
S21A(config-mst)#instance 1 vlan 10,30         //配置 instance 1(实例 1)并关联 Vlan
10 和 30
S21A(config-mst)#instance 2 vlan 20        //配置实例 2 并关联 Vlan 20
S21A(config-mst)#name region1              //配置域名称
S21A(config-mst)#revision 1                //配置版本（修订号）
```

（6）验证 MSTP 配置

```
S21A#show spanning-tree mst configuration //显示 MSTP 全局配置
```

第 2 步：配置接入层交换机 S21B

（1）开启生成树

```
S21B (config)#spanning-tree                //开启生成树
S21B (config)#spanning-tree mode mstp      //配置生成树模式为 MSTP
```

（2）创建 VLAN

```
S21B(config)#vlan 40    //创建 Vlan 40
```

（3）划分 VLAN 端口

```
S21B(config)#interface range fastethernet 0/3-22
S21B(config-if)#switchport access vlan 40 //分配端口 F0/3-22 给 Vlan 10
```

（4）配置 Trunk

```
S21B(config)#interface fastethernet 0/1
S21B(config-if)#switchport mode trunk      //定义 F0/1 为 trunk 端口
S21B(config)#interface fastethernet 0/2
S21B(config-if)#switchport mode trunk      //定义 F0/2 为 trunk 端口
```

（5）配置实例关联 VLAN

```
S21B(config)#spanning-tree mst configuration  //进入 MSTP 配置模式
S21B(config-mst)#instance 2 vlan 40           //配置实例 2 并关联 Vlan 20 和 40
S21B(config-mst)#name region1                 //配置域名称
S21B(config-mst)#revision 1                   //配置版本（修订号）
```

（6）验证 MSTP 配置

```
S21B#show spanning-tree mst configuration    // 显示 MSTP 全局配置
```

第 3 步：配置接入层交换机 S21C

（1）开启生成树

```
S21C (config)#spanning-tree   //开启生成树
```

```
S21C (config)#spanning-tree mode mstp          //配置生成树模式为 MSTP
```

（2）创建 VLAN

```
S21C(config)#vlan 10    //创建 Vlan 10
S21C(config)#vlan 20    //创建 Vlan 20
S21C(config)#vlan 30    //创建 Vlan 30
```

（3）划分 VLAN 端口

```
S21C(config)#interface range fastethernet 0/3-8
S21C(config-if)#switchport access vlan 10      //分配端口 F0/3-8 给 Vlan 10
S21C(config)#interface range fastethernet 0/9-15
S21C(config-if)#switchport access vlan 20      //分配端口 F0/9-15 给 Vlan 20
S21C(config)#interface range range fastethernet 0/16-22
S21C(config-if)#switchport access vlan 30      //分配端口 F0/16-22 给 Vlan 30
```

（4）配置 Trunk

```
S21C(config)#interface fastethernet 0/1
S21C(config-if)#switchport mode trunk      //定义 F0/1 为 trunk 端口
S21C(config)#interface fastethernet 0/2
S21C(config-if)#switchport mode trunk      //定义 F0/2 为 trunk 端口
```

（5）配置实例关联 VLAN

```
S21C(config)#spanning-tree mst configuration  //进入 MSTP 配置模式
S21C(config-mst)#instance 1 vlan 10,30        //配置 instance 1(实例 1)并关联 Vlan
10 和 30
S21C(config-mst)#instance 2 vlan 20           //配置实例 2 并关联 Vlan 20
S21C(config-mst)#name region1                 //配置域名称
S21C(config-mst)#revision 1                   //配置版本（修订号）
```

（6）验证 MSTP 配置

```
S21C#show spanning-tree mst configuration      //显示 MSTP 全局配置
```

第 4 步：配置接入层交换机 S21D

（1）开启生成树

```
S21D (config)#spanning-tree                    //开启生成树
S21D (config)#spanning-tree mode mstp          //配置生成树模式为 MSTP
```

（2）创建 VLAN

```
S21D(config)#vlan 10    //创建 Vlan 10
S21D(config)#vlan 20    //创建 Vlan 20
S21D(config)#vlan 30    //创建 Vlan 30
```

（3）划分 VLAN 端口

```
S21D(config)#interface range fastethernet 0/3-7
S21D(config-if)#switchport access vlan 10   //分配端口 F0/3-7 给 Vlan 10
```

```
S21D(config)#interface range fastethernet 0/8-12
S21D(config-if)#switchport access vlan 20   //分配端口 F0/8-12 给 Vlan 20
S21D(config)#interface range range fastethernet 0/13-17
S21D(config-if)#switchport access vlan 30   //分配端口 F0/13-17 给 Vlan 30
```

（4）配置 Trunk

```
S21D(config)#interface fastethernet 0/1
S21D(config-if)#switchport mode trunk     //定义 F0/1 为 trunk 端口
S21D(config)#interface fastethernet 0/2
S21D(config-if)#switchport mode trunk     //定义 F0/2 为 trunk 端口
```

（5）配置实例关联 VLAN

```
S21D(config)#spanning-tree mst configuration      //进入 MSTP 配置模式
S21D(config-mst)#instance 1 vlan 10,30            //配置 instance 1（实例 1）并关
联 Vlan 10 和 30
S21D(config-mst)#instance 2 vlan 20               //配置实例 2 并关联 Vlan 20
S21D(config-mst)#name region1                     //配置域名称
S21D(config-mst)#revision 1                       //配置版本（修订号）
```

（6）验证 MSTP 配置

```
S21D#show spanning-tree mst configuration         //显示 MSTP 全局配置
```

第 5 步：配置三层交换机 S35A

（1）开启生成树

```
S35A(config)#spanning-tree                //开启生成树
S35A (config)#spanning-tree mode mstp     //采用 MSTP 生成树模式
```

（2）创建 VLAN

```
S35A(config)#vlan 10
S35A(config)#vlan 20
S35A(config)#vlan 30
S35A(config)#vlan 40
```

（3）配置 Trunk

```
S35A(config)#interface fastethernet 0/1
S35A(config-if)#switchport mode trunk     //定义 F0/1 为 trunk 端口
S35A(config)#interface fastethernet 0/2
S35A(config-if)#switchport mode trunk     //定义 F0/2 为 trunk 端口
S35A(config)#interface fastethernet 0/3
S35A(config-if)#switchport mode trunk     //定义 F0/3 为 trunk 端口
S35A(config)#interface fastethernet 0/4
S35A(config-if)#switchport mode trunk     //定义 F0/4 为 trunk 端口
```

（4）配置端口聚合

```
S35A(config)#interface range fastethernet 0/5-6
```

```
S35A(config-if)#switchport mode trunk            //定义 F0/5-6 为 trunk 端口
S35A (config-int-range)#channel-group 1 mode on  //f0/5-6 端口聚合
```

（5）配置实例 1 的优先级

```
S35A (config)#spanning-tree mst 1 priority 4096   //配置交换机 S35A 在 instance 1 中的优先级为 4096 ，缺省是 32768，值越小越优先成为该 instance 中的 root switch
```

（6）配置实例与 VLAN 关联

```
S35A (config)#spanning-tree mst configuration     // 进入 MSTP 配置模式
S35A (config-mst)#instance 1 vlan 10,30      //配置实例 1 并关联 Vlan 10 和 30
S35A (config-mst)#instance 2 vlan 20,40      //配置实例 2 并关联 Vlan 20 和 40
S35A (config-mst)#name region1               //配置域名为 region1
S35A (config-mst)#revision 1                 //配置版本（修订号）
```

（7）验证 MSTP 配置

```
S35A#show spanning-tree mst configuration
```

第 6 步：配置三层交换机 S35B

（1）开启生成树

```
S35B(config)#spanning-tree                   //开启生成树
S35B (config)#spanning-tree mode mstp        //采用 MSTP 生成树模式
```

（2）创建 VLAN

```
S35B(config)#vlan 10
S35B(config)#vlan 20
S35B(config)#vlan 30
S35B(config)#vlan 40
```

（3）配置 Trunk

```
S35B(config)#interface fastethernet 0/1
S35B(config-if)#switchport mode trunk     //定义 F0/1 为 trunk 端口
S35B(config)#interface fastethernet 0/2
S35B(config-if)#switchport mode trunk     //定义 F0/2 为 trunk 端口
S35B(config)#interface fastethernet 0/3
S35B(config-if)#switchport mode trunk     //定义 F0/3 为 trunk 端口
S35B(config)#interface fastethernet 0/4
S35B(config-if)#switchport mode trunk     //定义 F0/4 为 trunk 端口
```

（4）配置端口聚合

```
S35B(config)#interface range fastethernet 0/5-6
S35B(config-if)#switchport mode trunk           //定义 F0/5-6 为 trunk 端口
S35B (config-int-range)#channel-group 1 mode on //f0/5-6 端口聚合
```

（5）配置实例 2 的优先级

```
S35B (config)#spanning-tree mst 2 priority 4096   //配置交换机 S35A 在 instance
```

```
1 中的优先级为 4096,缺省是 32768,值越小越优先成为该 instance 中的 root switch
```

（6）配置实例与 VLAN 关联

```
S35B (config)#spanning-tree mst configuration   //进入 MSTP 配置模式
S35B (config-mst)#instance 1 vlan 10,30      //配置实例 1 并关联 Vlan 10 和 30
S35B (config-mst)#instance 2 vlan 20,40      //配置实例 2 并关联 Vlan 20 和 40
S35B (config-mst)#name region1               //配置域名为 region1
S35B (config-mst)#revision 1                 //配置版本（修订号）
```

（7）验证 MSTP 配置

```
S35B#show spanning-tree mst configuration
```

第 5 步：核心交换机 3SWA 设置 VLAN 管理地址，作为相应 VLAN 的网关：

```
S35A(config)#interface vlan 10
S35A(config-if)#ip address 192.168.10.2 255.255.255.0 //配置 VLAN10 的 IP 地址
S35A(config)#interface vlan 20
S35A(config-if)#ip address 192.168.20.2 255.255.255.0 //配置 VLAN20 的 IP 地址
S35A(config)#interface vlan 30
S35A(config-if)#ip address 192.168.30.2 255.255.255.0 //配置 VLAN30 的 IP 地址
S35A(config)#interface vlan 40
S35A(config-if)#ip address 192.168.40.2 255.255.255.0 //配置 VLAN40 的 IP 地址
```

第 6 步：核心交换机 3SWB,设置 VLAN 管理地址，作为相应 VLAN 的网关：

```
S35B(config)#interface vlan 10
S35B(config-if)#ip address 192.168.10.3 255.255.255.0 //配置 VLAN10 的 IP 地址
S35B(config)#interface vlan 20
S35B(config-if)#ip address 192.168.20.3 255.255.255.0 //配置 VLAN20 的 IP 地址
S35B(config)#interface vlan 30
S35B(config-if)#ip address 192.168.30.3 255.255.255.0 //配置 VLAN10 的 IP 地址
S35B(config)#interface vlan 40
S35B(config-if)#ip address 192.168.40.3 255.255.255.0 //配置 VLAN10 的 IP 地址
```

第 7 步：配置交换机 S35A 的 VRRP

```
S35A(config)#interface vlan 10
S35A(config-if)#standby 1 ip 192.168.10.254      //配置虚拟 IP，即 VLAN10 的虚拟网关
S35A(config-if)#standby 1 preempt     //设为抢占模式:正常状况下,VLAN10 的数据由 35A 传输.当 35A 发生故障时,则由 35B 担负起传输任务.若不配置抢占模式，当 35A 恢复正常后，数据仍由 35B 传输;配置抢占模式后,正常后的 35A 会再次夺取对 VLAN10 的控制权.
S35A(config-if)#standby 1 priority 254      //VLAN10 的 standby 优先级设为 254,在同一个 VLAN 中，优先级较高的设备成为 master，较低的设备成为 backup， master 的虚拟网关生效。Standby 默认优先级为 100.
S35A(config-if)#exit
S35A(config)#interface vlan 20
S35A(config-if)#standby 2 ip 192.168.20.254   //配置虚拟 IP，即 VLAN20 的虚拟网关
S35A(config-if)#standby 2 priority 120    //VLAN20 的 standby 优先级设为 120,
```

```
Standby 默认优先级为 100。
    S35A(config-if)#exit
    S35A(config)#interface vlan 30
    S35A(config-if)#standby 1 ip 192.168.30.254      //配置虚拟 IP，即 VLAN30 的虚
拟网关
    S35A(config-if)#standby 1 preempt
    S35A(config-if)#standby 1 priority 254
    S35A(config-if)#exit
    S35A(config)#interface vlan 40
    S35A(config-if)#standby 2 ip 192.168.40.254
    S35A(config-if)#standby 2 priority 120
    S35A(config-if)#exit
```

第 8 步：配置交换机 S35B 的 VRRP

```
    S35B(config)#interface vlan 10
    S35B(config-if)#standby 1 ip 192.168.10.254    //配置虚拟 IP
    S35B(config-if)#standby 2 priority 120
    S35B(config-if)#exit
    S35B(config)#interface vlan 20
    S35B(config-if)#standby 2 ip 192.168.20.254    //配置虚拟 IP
    S35B(config-if)#standby 2 priority 254 //VLAN20 的 standby 优先级设为 254
    S35B(config-if)#standby 2 preempt              //设为抢占模式
    S35B(config-if)#exit
    S35B(config)#interface vlan 30
    S35B(config-if)#standby 1 ip 192.168.30.254
    S35B(config-if)#standby 1 priority 120
    S35B(config-if)#exit
    S35B(config)#interface vlan 40
    S35B(config-if)#standby 2 ip 192.168.40.254    //配置虚拟 IP，即 VLAN40 的虚拟网关
    S35B(config-if)#standby 2 preempt              //设为抢占模式
    S35B(config-if)#standby 2 priority 254 //VLAN40 的 standby 优先级设为 254
    S35B(config-if)#exit
```

第 9 步：给三层交换机和路由器配置相应 IP 地址

（1）配置交换机 S35A 的接口 IP 地址

```
    S35A(config)#interface f0/7
    S35A(config-if)#no switchport          //让交换机端口工作在路由模式
    S35A(config-if)#ip address 172.16.1.1 255.255.255.0
```

（2）配置交换机 S35B 的接口 IP 地址

```
    S35B(config)#interface f0/7
    S35B(config-if)#no switchport          //让交换机端口工作在路由模式
    S35B(config-if)#ip address 172.16.2.1 255.255.255.0
```

（3）配置路由器 R0 的接口 IP 地址

```
R0(config)#interface f0/3
R0(config-if)#ip address 172.16.1.2 255.255.255.0
R0(config)#interface f0/2
R0(config-if)#ip address 182.100.1.2 255.255.255.252
R0(config)#interface f0/4
R0(config-if)#ip address 172.16.2.2 255.255.255.0
```

第 10 步：在交换机 3SWA、3SWB、R0 上配置静态路由实现网络互通

（1）配置交换机 S35A 的默认路由

```
3SWA>en
3SWA#conf t
3SWA(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.2
```

（2）配置交换机 S35B 的默认路由

```
3SWB>en
3SWB#conf t
3SWB(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2
```

（3）配置出口路由

```
R0>en
R0#conf t
R0(config)#ip route 0.0.0.0 0.0.0.0  182.100.1.1   // 182.100.1.1 为电信端的 IP 地址
```

（4）配置路由器的回指路由

配置路由器的回指路由时，回指到每个内部网络的路由均需要配置两条静态路由，网络正常情况下路由器选择管理距离小的转发数据，管理距离大的为备用路由。以防止当交换机 S35A 或 S35B 其中一个出现故障时，路由器会选择管理距离大的备用路由来转发数据，网络仍然能够正常运行。

```
R0(config)#ip route 192.168.10.0 255.255.255.0 172.16.1.1 1
R0(config)#ip route 192.168.10.0 255.255.255.0 172.16.2.1 2
R0(config)#ip route 192.168.20.0 255.255.255.0 172.16.2.1 1
R0(config)#ip route 192.168.20.0 255.255.255.0 172.16.1.1 2
R0(config)#ip route 192.168.30.0 255.255.255.0 172.16.1.1 1
R0(config)#ip route 192.168.30.0 255.255.255.0 172.16.2.1 2
R0(config)#ip route 192.168.40.0 255.255.255.0 172.16.2.1 1
R0(config)#ip route 192.168.40.0 255.255.255.0 172.16.1.1 2
```

项目测试

步骤一：在办公楼计算机的 IP 地址，VLAN10 下所属 A 机的 IP 地址为 192.168.10.10/24，使用 tracert 命令测试外网口 IP182.100.1.2，跟踪数据包路由，发现数据包路由将是 SA21→SW35A→R0，如图 4-17 所示。

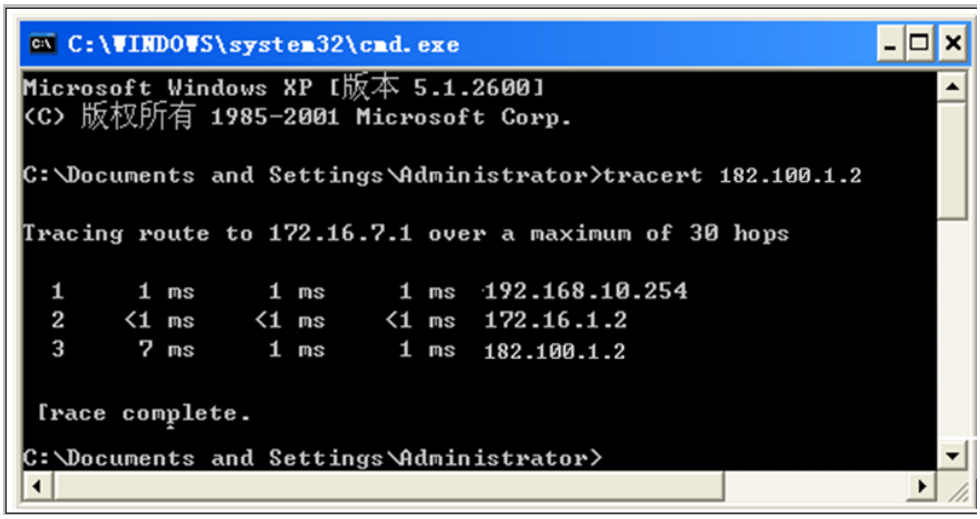


图 4-17　内部主机路由跟踪

步骤二：关闭 3SWA 核心，再次使用命令 tracert 再次跟踪到出口的路由，发现这时路由发生了改变 SA21→SW35B→R0，如图 4-18 所示。

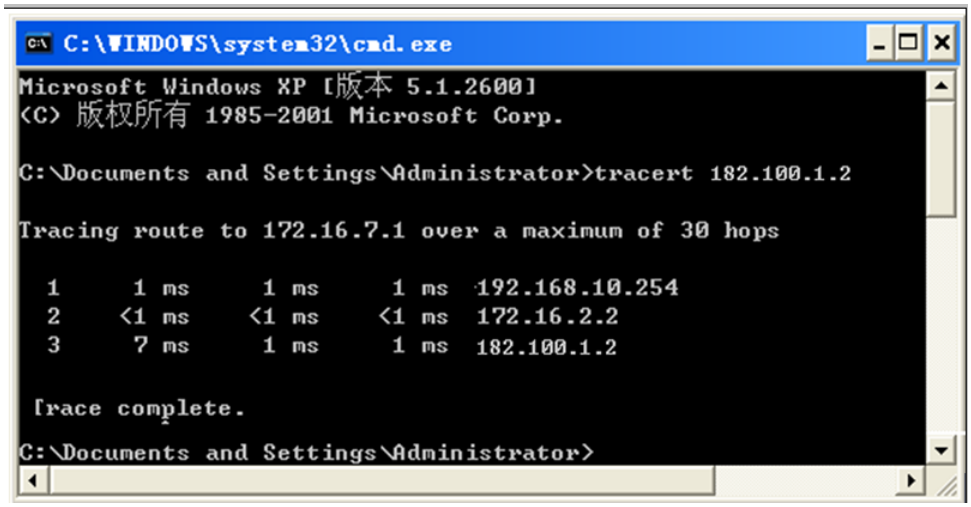


图 4-18　内部主机路由跟踪

认证测试

一、选择题

1．下列哪些命令设置端口模式为链路汇聚模式（　　）。

A．Write　　B．switchport mode trunk

C．Write memory　　D．switchport mode access

2．VRRP 协议提供了三种认证方式，（　　）可以根据不同的网络环境使用不同的认证方式。

A．无认证　　B．简单字认证　　C．MD5 认证　　D．Hash 认证

3．下列哪条命令是显示生成树网络参数的命令（　　）。

A．ipconfig　　B．show interface Ethernet 0/0/1

C．ipconfig/all　　D．show spanning-tree

4.（　　）层作为整个网络系统的核心，其主要功能是高速、可靠地进行数据交换（　　）。

A．核心层　　B．汇聚层　　C．网络层　　D．接入层

5．主机位全 0 的地址是（　　）。

A．广播地址　　B．网络地址　　C．本地地址　　D．本网络的本台地址

6．在生成树协议发展过程中，不断克服以前的缺陷，并不断开发新的功能。按照功能的改进情况，我们把生成树的发展过程划分为三代，第三代生成树协议是指（　　）。

A．STP/RSTP　　B．PVST/PVST+　　C．MISTP/MSTP　　D．VRRP

7．下面（　　）命令可以正确地启用生成树协议。

A．spanning-tree　　B．spanning-tree mode

C．spanning-tree configure　　D．show spanning-tree

二、简答题

1．简述网络通常使用的分层结构，每层具有哪些功能？

2．简述 IPv4 地址可以分为哪几类，每一类的范围是多少？

3．简述 VRRP 协议工作的三种状态？

4．描述生成树的工作过程？

5．描述 VRRP 的工作过程？

项目五　碧宏电子有限公司网络配置与管理（ACL）

项目背景

碧宏电子有限公司是一家小型电子企业，目前采用无纸化网络办公，网络架构是由一台普通路由器接入互联网作为上网出口路由器，在路由器下串联了 2 台 24 口的“傻瓜”交换机作为公司 3 个部门的计算机接入上网组成的简单网络。公司的部门分别为财务部、市场部、研发部，每个部门的人数均不到 20 人，公司整个内部网络都在 192.168.1.0/24 网段内。该网络的拓扑结构如图 5-1 所示。

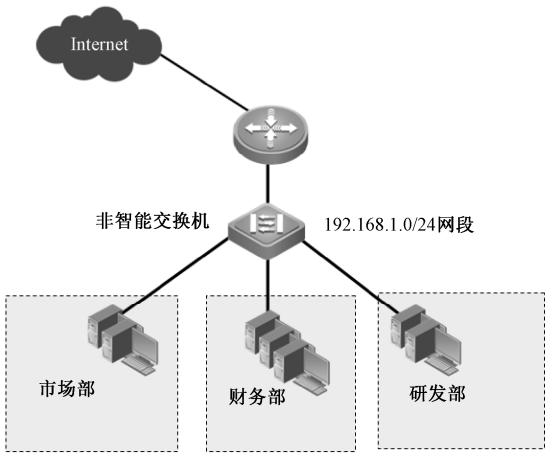


图 5-1　网络拓扑图

自从该公司网络建成以后，就遇到一些麻烦事。公司经理一会儿向老板抱怨说互联网开通后，员工上班时间就知道“泡网”影响工作效率；还有随着员工增加即将面临交换机端口不够用；随着公司业务的增长，需要一台放置公司网站的服务器和一台供员工和客户下载资料的服务器；财务部一会儿又向老板抱怨说研发部的员工访问了财务部共享资料，看了一些保密数据；老板听到员工们抱怨的问题后，下决心要改善解决这些问题，但是由于现在的网络环境是请人临时搭建的，没有意识到后续会存在问题，而且公司为节省开支，并没有聘请专职的网络管理员。为了解决这些“高深”的问题，老板不得不聘请了一家网络技术公司的张工程师来对公司的网络进行改造。

项目分析

网络技术公司的张工程师，在对现有公司进行详细的了解后，进行了以下分析：

分析一：财务部抱怨研发部的员工看了不该看的数据，所以现在要实现部门间的访问安全，财务部不允许研发部访问，其他部门访问将被允许。

分析二：现在公司的服务器群有 FTP 服务，FTP 供财务部专用，其他部门不可使用。现在需要保护公司内部服务器访问安全，限制部门访问内容。

分析三：公司领导抱怨员工上班时间就知道“泡网”，影响工作效率。现在需要保证公司上班时间的工作效率，控制员工上网时间及访问内容。

项目方案

由于当前使用的“傻瓜”交换机不具备 VLAN 和 ACL 访问控制列表功能。所以需要淘汰现今网络中的二层“傻瓜”交换机，购置 l 台新的三层交换机和 4 台二层交换机。通过在三层交换机上进行相关的配置来实现公司的需求。首先要在三层交换机上划分 4 个 VLAN 分别给不同部门，然后再配置 ACL 限制部门之间访问。部署完毕后的新网络拓扑如图 5-2 所示。

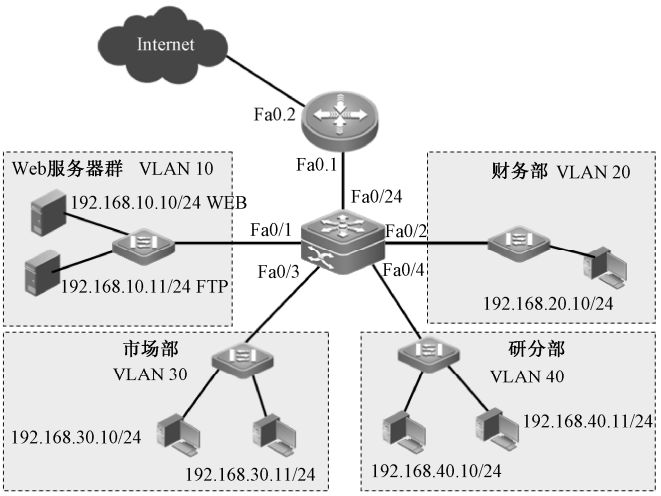


图 5-2　新网络拓扑图

根据碧宏电子有限公司重新部署和调整的公司网络，通过一台路由器接入到互联网。在网络核心使用一台思科 SF300-24 三层交换机，部门计算机接入的二层交换机为可管理的思科 SF200E-24 交换机，在公司内部使用了 VLAN 技术，按照功能的不同分为了 4 个 VLAN。分别是服务器群（VLAN10）、财务部（VLAN20）、市场部（VLAN30）、研发部门（VLAN40），如表 5-1 所示。在出口路由器上 Fa0/1 接公司内部网，通过 F0/2 连接到 Internet。

表 5-1　VLAN 号

部　　门	VLAN 号	网　　段
服务器群	VLAN10	192.168.10.0/24
财务部	VLAN20	192.168.20.0/24
市场部	VLAN30	192.168.30.0/24
研发部	VLAN40	192.168.40.0/24

知识准备

1．访问控制列表概述

访问控制列表是一种实施在交换机与路由器上的一种技术，其主要目的是对网络通信的数据流量进行过滤，从而实现各种访问控制的需求。例如，你可以将 ACL 访问列表上设置只

允许某些特定的计算机可以访问网络中的 WWW 资源，而却不允许其他主机访问。通过恰当的配置可以实施几乎任何可以想象到的安全策略提供网络的安全性。

ACL 技术通过数据包中的五元组（IP 地址、目标 IP 地址、协议号、源端口号、目标端口号）来区分特定的数据流，并对匹配预设的 ACL 规则采取相应的行为，允许（Permit）或拒绝（Deny）数据通过，从而实现对网络的安全控制。

创建访问控制列表同编写一系列 if-then 语句非常相似，如果满足给定的条件，则执行给定的操作；如果指定的条件不满足，不做任何操作，继续测试下一个语句。访问列表语句基本上是对包进行比较、分类，然后根据条件实施操作的包过滤器。列表一旦建立，可以应用到任何端口输入或输出方向的流量上。应用访问列表后，路由器会分析沿特定方向通过哪个接口的每个包，并执行相应的操作。

下面是一些将数据包和列表进行比较时应遵循的重要规则：

（1）通常，按顺序比较访问列表的每一条，例如，从第一条开始，然后转到第二条，第三条等。

（2）比较访问列表的各条，直到找到匹配的一条。一旦数据包与访问列表的某一条匹配，将遵照规定执行工作，不再进行后续的条目进行比较。

（3）在每个访问列表的最后一条默认是隐含“Deny（拒绝）”语句，意味着如果数据包与访问列表中的所有条都不匹配，将被丢弃。

使用访问列表过滤 IP 包时，这里的每一条规则都具有隐含功能。所以请记住，要创建有效的访问列表，需要多进行一些练习。

2．标准访问控制列表

标准访问控制列表中，对数据包的检查过滤是仅依 IP 数据包的源 IP 地址。这意味着标准的访问控制列表只能允许或者拒绝整个源 IP 段的全部协议，而不能区分 IP 流量的类型，如 WWW、Telnet、UDP 等服务。标准访问控制列表使用的 ACL 号为 1～99。

编号访问控制列表是在路由器上建立的访问控制列表，其编号取值范围 0～99 之间整数值。标准访问控制列表再根据源 IP 地址过滤流量，这个 IP 地址可以是一台主机、整个网络或者特定网络上的特定主机。

当交换机收到一个数据包时，根据该数据包的源 IP 地址从访问控制列表上面第一条语句开始逐条检查各条语句。如果检查到匹配语句，根据语句中是允许或禁止流量通过来处理该数据包；如果检查到最后一条语句还没有匹配的语句，则该数据包被丢弃。

注意：*在标准或扩展访问列表的末尾，总有一个隐含的 deny all。这意味着如果该数据包原地址与任何允许语句不匹配，则隐含的 deny all 将会禁止该数据包通过。*

（1）定义访问控制列表，所有访问控制列表都是在全局配置模式下设置的，IP 标准访问列表的格式如下：

```
Switch(config)#access-list access-list number {permit/deny} source {source mask}
```

其中，access-list number 是访问列表序号，IP 标准访问列表的序号是 1～99。

Permit/deny 表示访问控制列表是允许还是禁止满足条件的数据包通过。

Source 是要被过滤数据包的源 IP 地址。

Source mask 是通配符掩码，1 表示不检查位，0 表示必须匹配位。

其他可提供选项参数是 any 和 host，它们可用于 permit 和 deny 语句之后来说明任何主机。

这两条命令简化了语句，因为它们不需要一个通配符掩码。Any 命令等于通配符掩码 255.255.255.255，host 命令等于通配符掩码 0.0.0.0。

【例 5-1】只允许研发部可以访问财务部。定义访问控制列表 1 允许来自网络 192.168.10.0 的流量通过，如图 5-3 所示。

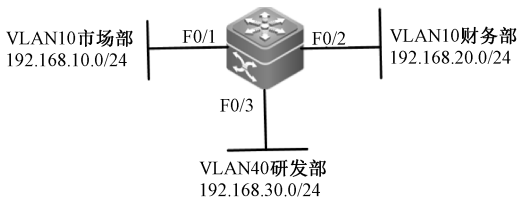


图 5-3　示例图

```
Switch (config)#access-list 1 permit 192.168.10.0 0.0.0.255
Switch(config)#interface fastethernet 0/2
Switch(config-if)#ip access-group 1 out
```

【例 5-2】拒绝研发部访问财务部，其他部门一律允许。定义访问控制列表 2 特别禁止来自网络 192.168.10.0 的流量通过，如图 5-4 所示。

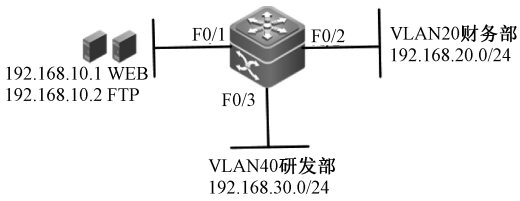


图 5-4　示例图

```
Switch (config)# access-list 2 deny 192.168.30.0 0.0.0.255
Switch (config)#access-list 2 permit any
Switch(config)#interface fastethernet 0/2
Switch(config-if)#ip access-group 2 out
```

【例 5-3】限制所有部门访问服务器群主机 Web，服务器群其他主机不限制。定义访问控制列表 3 拒绝特定主机 192.168.10.1 的流量通过，但允许其他的所有主机的流量通过，如图 5-5 所示。

```
Switch (config)#access-list 3 deny host 192.168.10.1
Switch (config)#access-list 3 permit any
Switch(config)#interface fastethernet 0/1
Switch(config-if)#ip access-group 3 out
```

【例 5-4】定义访问控制列表 4 拒绝从 192.168.0.0～192.168.255.255 的所有流量通过，但允许 192.167.0.0～192.167.255.255 的流量通过，如图 5-5 所示。

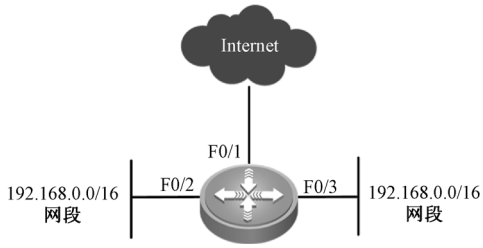


图 5-5 示例图

```
Switch (config)#access-list 4 deny 192.168.0.0 0.0.255.255
Switch (config)#access-list 4 permit 192.167.0.0 0.0.255.255
Switch (config)#interface fastethernet 0/1
Switch (config-if)#ip access-group 4 out
```

（2）应用访问控制列表。一旦建立了标准访问控制列表，需要将它们应用到交换机的一个端口上。应用到一个接口上可以选择入站（IN）或出站（OUT）两个方向。对于某一个接口，当要将从设备外的数据经接口流入设备内时做访问控制，就是入站（IN）应用；当要将从设备内的数据经接口流出设备时做访问控制，就是出站（OUT）应用。交换机一个接口一个方向上只能应用一个访问控制列表。

【例 5-5】将访问控制列表 1 应用到交换机的接口 Fastethernet 0 的入站方向上。

```
Switch(config)#interface fastethernet 0
Switch(config-if)#ip access-group 1 in
Switch(config-if)#end
```

（3）查看访问控制列表。配置完 IP 访问列表后，你可以通过 access-lists 命令来验证写入的 ACL 条目是否正确。

【例 5-6】查看交换的访问控制列表。

```
S#show access-list
```

3．扩展访问控制列表

扩展访问控制列表中，对数据包的检查过滤依据更为丰富，可以检查 IP 包头中的第 3 层和第 4 层包头中的字段。扩展的 ACL 和标准的 ACL 的应用规则相同，区别是在于扩展 ACL 对数据检查的依据是更丰富一些。扩展 ACL 可以检查的元素有：源 IP 地址、目标 IP 地址、协议、源端口号、目标端口号。扩展访问控制列表使用的 ACL 号为 100 到 199。

1．扩展访问控制列表简述。扩展编号访问控制列表同标准编号访问控制列表一样，也是在交换机或者路由器上创建的。其编号范围 100～199。扩展 IP 访问控制列表可以基于数据包源 IP 地址、目的地址、协议及端口号等信息来过滤流量。

当交换机收到一个数据包时，交换机根据数据包的源 IP 地址、目的地址、协议及端口号等从访问控制列表中自上而下检查控制语句。如果检查到与一条 permit 语句匹配，则允许该数据包通过；如果检查到与一条 deny 语句匹配，则该数据包被丢弃；如果检查到最后一条语句后还没有找到匹配的，则该数据包被将被丢弃。一旦控制列表允许数据包通过，交换机将数据包的目标网络地址与交换机上的内部路由表进行选择路径，就可以把数据包路由到它的

目的地址。

2．配置扩展访问控制列表和标准访问控制列表一样，扩展 IP 访问控制列表页在全局配置模式下输入。扩展 IP 访问控制列表配置命令格式如下：

```
SW(config)#access-list listnumber{permit/deny} protocol source-address source-wildcard-mask destination-address destination-wildcard-mask {operator operand}
```

listnumber 为规则序号，扩展访问控制列表的规则序号范围为 100～199。

permit 和 deny 标准允许或者禁止满足该规则的数据包通过。

protocol 可以指定为 0～255 之间的任一协议号，对于常见协议（如 IP、TCP 和 UDP）。

operator operand 用于指定端口范围，默认全部端口号为 0～65535，只有 TCP 和 UDP 协议需要指定端口范围。支持的操作符及其语法如表 5-2 所示。

表 5-2　操作符及语法

操作符及语法	意　义
Eg portnumber	等于端口号 portnumber
Gt portnumber	大于端口号 portnumber
Lt portnumber	小于端口号 portnumber
Neg portnumber	不等于端口号 portnumber
Range portnumber1 portnumber2	介于端口号 portnumber1 和 portnumber2 之间

在指定 portnumber 时，对于部分常见的端口号，可以用相应的助记符来代替其实际数字，常用的 TCP 端口号和 UDP 端口号如表 5-3 所示。

表 5-3　常用的端口号

名　称	TCP/UDP	端　口　号
域名系统（DNS）	TCP/UDP	53
超文本传输协议（HTTP）	TCP	80
简单邮件传输协议（SMTP）	TCP	25
邮局协议（POP）	UDP	110
远程登录（Telnet）	TCP	23
动态主机配置协议（DHCP）	UDP	67
文件传输协议（FTP）	TCP	20，21

3．应用访问控制列表。在交换机接口上应用访问控制列表，如表 5-4 所示。

表 5-4　应用访问控制列表

操 作 说 明	操 作 命 令
指定接口上过滤接收报文的规则	ip access-group listnumber in
取消接口上过滤接收报文的规则	no ip access-group listnumber in
指定接口上过滤接收报文的规则	ip access-group listnumber out
取消接口上过滤接收报文的规则	no ip access-group listnumber out

参数 in/out 表示是入站还是出站。如果你想访问列表对两个方向都应用，则两个参数都要加上，一个表示入站，一个表示出站。对于每个协议的每个接口的每个方向，还能应用一个访问列表。

【例 5-7】在交换机上配置访问控制列表，实现只允许财务部 192.168.20.0 网段的主机向服

务器群 192.168.10.0 网段的主机发送 WWW 报文，禁止其他报文通过，如图 5-6 所示。

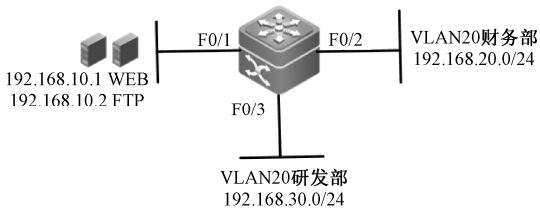


图 5-6　示例图

```
    SW(config)#access-list 100 permit tcp 192.168.20.0 0.0.0.255 192.168.10.0
0.0.0.255 eq www
    SW(config)#intface fastethernet 0/1
    SW(config-if)#ip access-group 100 out
    SW(config-if)#end
    SW#show access-list
```

4．基于命名访问控制列表可以是命名的标准访问控制列表和标准的访问控制列表，命名访问控制列表可以使用字母-数字串（名字）表示，而不是仅限于数字表示。配置标准命名访问控制列表和扩展的命名列表的命令格式如下：

（1）标准命名访问控制列表

```
    Switch#configure terminal
```

创建标准的命名访问控制列表：

```
    Switch(config)#ip access-list standard {name}
```

定义命名访问控制列表定义列表条件：

```
    Switch(config-std-nacl)#deny/permit {source source-wildcard | host source | any}
    Switch(config-stan-nacl)#exit
```

例如，命名标准访问控制列表：

```
    Switch(config)#ip access-list standard test
    Switch(config-std-nacl)#deny 192.168.1.0 0.0.0.255
    Switch(config-std-nacl)#deny host 192.168.2.1
    Switch(config-std-nacl)#permit any
    Switch(config- std -nacl)#exit
    Switch#show access-lists      //如图 5-7 所示
```

```
Standard IP access list test
    20 deny   192.168.2.1
    10 deny   192.168.1.0, wildcard bits 0.0.0.255
    30 permit any
```

图 5-7　查看访问控制列表

（2）扩展命名访问控制列表

```
    Switch#configure terminal
```

创建扩展的命名访问控制列表：

```
Switch(config)#ip access-list extended {name}
```

定义命名访问控制列表定义列表条件：

```
Switch(config-ext-nacl)#deny/permit protocol { any | source source-wildcard }
[ port ] { any | destination destination-wildcard } [ port ]  [ time-range-name ]
```

例如，命名扩展访问控制列表：

```
Switch(config)#ip access-list extended test
Switch(config-ext-nacl)# deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
Switch(config-ext-nacl)# deny tcp 192.168.1.0 0.0.0.255 host 192.168.3.1 eq www
Switch(config-ext-nacl)# permit ip any any
Switch(config- std -nacl)#exit
Switch#show access-lists    //如图 5-8 所示
```

```
Switch#show access-lists
Extended IP access list test
    10 deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
    20 deny tcp 192.168.1.0 0.0.0.255 host 192.168.3.1 eq www
    30 permit ip any any
```

图 5-8　查看访问控制列表

对于使用数字表示的访问控制列表语句，管理员如果想要单独删除访问控制列表的一条一句是不能实现的，它只能把整个 IP 访问控制列表删除后再重写，变更灵活性小。而对于命名访问控制列表可以从访问列表中特定删除单个 ACL 语句，也可以增加一条语句在特定语句的前后顺序位置，使用名称来命名的访问控制列表管理员可以更加直观地了解该访问控制列表的作用。数字访问控制列表和命名访问控制列表的区别如下。

数字标准访问控制列表：

```
Switch(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Switch(config)#access-list 1 permit 192.168.2.0 0.0.0.255
Switch(config)#access-list 1 permit 192.168.4.0 0.0.0.255
Switch(config)#access-list 1 deny any
```

命名标准访问控制列表：

```
Switch(config)#ip access-list standard test
Switch(config-std-nacl)#permit 192.168.1.0, wildcard bits 0.0.0.255
Switch(config-std-nacl)#permit 192.168.2.0, wildcard bits 0.0.0.255
Switch(config-std-nacl)#permit 192.168.4.0, wildcard bits 0.0.0.255
Switch(config-std-nacl)#deny any
```

【例 5-8】如管理员在配置访问控制列表完毕后发现自己错误地配置了一条允许 192.168.4.0/24 的语句。在数字标准访问控制列表中如果想要删除该条语句，只能全部删除后，重新配置访问控制列表。然而在命名访问控制列表中可以特定删除 192.168.4.0/24 语句，命令如下：

```
Switch#show access-lists //如图 5-9 所示
```

```
Switch#show access-lists
Standard IP access list test
    10 permit 192.168.1.0, wildcard bits 0.0.0.255
    20 permit 192.168.2.0, wildcard bits 0.0.0.255
    30 permit 192.168.4.0, wildcard bits 0.0.0.255
    40 deny   any
```

图 5-9　查看访问控制列表

命名列表中每条语句都有一个序号，图中可以看到 permit 192.168.4.0 0.0.0.255 的序号是 30。

```
Switch#configure terminal
Switch(config)#ip access-list standard test
Switch(config-std-nacl)#no 30
Switch(config-std-nacl)#exit
Switch#show access-lists   //如图 5-10 所示
```

```
Switch#show access-lists
Standard IP access list test
    10 permit 192.168.1.0, wildcard bits 0.0.0.255
    20 permit 192.168.2.0, wildcard bits 0.0.0.255
    40 deny   any
```

图 5-10　查看访问控制列表

图中所示命名访问控制列表中的 permit 192.168.4.0，Wildcard bits 0.0.0.255 已经被删除。

【例 5-9】如管理员在配置访问控制列表完毕后发现自己遗漏了一条允许 192.168.3.0/24 的语句，后面已经配置了 deny any 语句，所以遗漏的语句只能配置在 deny any 语句前面。在数字访问控制列表中无法实现语句添加到指定的顺序，只能删除后重新配置。然而在命令访问控制列表中可以添加语句到特定的位置，命令如下：

```
Switch#show access-lists   //如图 5-11 所示
```

```
Switch#show access-lists
Standard IP access list test
    10 permit 192.168.1.0, wildcard bits 0.0.0.255
    20 permit 192.168.2.0, wildcard bits 0.0.0.255
    30 permit 192.168.4.0, wildcard bits 0.0.0.255
    40 deny   any
```

图 5-11　查看访问控制列表

命名访问列表中执行的顺序是通过序号来判断先后顺序的，如图 5-12 结果所示，只要添加允许 192.168.3.0/24 的语句在 40 序号前即可。

```
Switch#configure terminal
Switch(config)#ip access-list standard test
Switch(config-std-nacl)#35 permit 192.168.3.0 0.0.0.255
Switch(config-std-nacl)#exit
Switch#show access-lists
```

```
Switch#show access-lists
Standard IP access list test
    10 permit 192.168.1.0, wildcard bits 0.0.0.255
    20 permit 192.168.2.0, wildcard bits 0.0.0.255
    30 permit 192.168.4.0, wildcard bits 0.0.0.255
    35 permit 192.168.3.0, wildcard bits 0.0.0.255
    40 deny   any
```

图 5-12　查看访问控制列表

如图 5-12 中结果所示添加了一条序号为 35 允许 192.168.3.0/24 的语句。

5．基于时间的 ACL 功能使管理员可以依据时间来控制用户对网络资源的访问，即可以根据时间来禁止/允许用户访问网络资源。为了实现基于时间的 ACL 功能，必须首先创建一个

time-range 接口来指明时间与日期。与其他接口一样，time-range 接口是通过名称来表示的。然后，就将 time-range 接口对应的 ACL 关联起来。IP 扩展访问控制列表 ACL 允许与 time-range 的关联。

（1）校正交换机时钟。为了有效地实现基于时间的访问控制列表功能，有必要校正交换机的时钟。具体操作如下：

设置系统时钟（时间及日期）：

```
SW#clock set hh:mm:ss date month year or clock set hh:mm:ss month date year
```

依据当前系统时钟设置更新路由器实时时钟：

```
SW#clock update-calendar
```

（2）创建并定义 time-range 接口。创建时间接口，并定义时间控制范围，具体操作如下：

进入全局配置模式：

```
SW#config terminal
```

创建/进入指定名称的 time-range 接口：

```
SW(config)#time-range time-range-name
```

进入 time-range 配置模式，设置限制的时间段。其中只允许配置一个 absolute 规则，但允许多个 periodic 规则并存：

```
SW(config-time-range)#absolute {start time date} {end time date} and/or periodic days-of -the-week hh:mm to {days-of-the-week} hh:mm
```

退出 time-rang 配置模式：

```
SW(config-time-range)#exit
```

（3）关联 time-range 接口与 ACL。只允许扩展访问控制列表 ACL 关联 time-range 接口，具体操作如下：

进入全局配置模式：

```
SW#config terminal
```

设置扩展的 ACL 关联 time-range 时间范围：

```
SW(config)#access-list {permit/deny} protocol srce-address src-wildcard desti-address desti-wildcard {time-range time-range-name}
```

退出全局配置模式：

```
SW(config)#exit
```

（4）在交换机接口上应用基于时间的 ACL，和其他类型的 ACL 应用方法一致，这里不再阐述。

（5）监控与维护。Time-range 接口指定时间是以交换机系统本地时间为准的。在使用基于时间的 ACL 功能之前，必须确认设备提供了可靠正确的时钟。

Time-range 接口上允许配置多条 periodic 规则，在 ACL 进行匹配时，只要能匹配任意一条 periodic 规则即认为匹配成功，而不是要求必须同时匹配多条 periodic 规则。

Time-range 接口只允许配置一条 absolute 规则。

Time-range 允许 absolute 规则与 periodic 规则共存，此时，ACL 必须首先匹配 absolute 规则，然后再匹配 periodic 规则。

如果 ACL 关联的 Time-range 接口不存在，系统就认为 ACL 已经在时间上匹配，即忽略时间因素。

【例 5-10】在交换机上配置基于时间的访问控制列表，实现所有部门访问互联网的 UDP 被限制在 2013 年 1 月 1 日上午 8:00～2013 年 12 月 31 下午 6:00 之间的周末（星期六与星期日）可以发送，如图 5-13 所示。

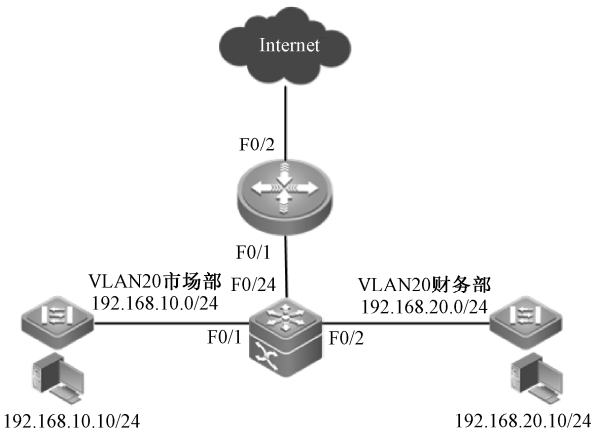


图 5-13 示例图

```
SW#confg terminal
SW(config)#time-range test
SW(config-time-range)#absolute start 8:00 1 january 2013 end 18:00 31 December
2013
SW(config-time-range)#periodic weekends 00:00 to 23:59
SW(config-time-range)#exit
SW(config)#access-list 100 permit udp any any time-range test
SW(config)#interface fastethernet 0/24
SW(config-if)#ip access-group 100 out
SW(config-if)#end
```

【例 5-11】在交换机上配置基于时间的访问控制列表，仅允许所有部门在星期一、星期二、与星期五的上午 9:00～下午 5:00 之间浏览互联网网页，接收目的端口为 80（www）的 TCP 报文。

```
SW#config terinal
SW(config)#time-range test
SW(config-time-range)#periodic Monday Tuesday Friday 9:00 to 17:00
SW(config-time-range)#exit
```

```
SW(config)#access-list 100 permit tcp any any eq www time-range test
SW(config)#interface fastethernet 0/24
SW(config-if)#ip access-group 100 out
SW(config-if)#end
SW#
```

项目实施

任务一　实现部门间的访问安全

任务描述

你是该公司的网络管理员，公司的服务器群、财务部、市场部和研发部分别属于不同的 4 个网段，4 个部门之间通过三层交换机进行信息传递，为了安全，公司领导要求你对网络数据流量进行控制，实现财务部只允许被市场部访问，其他部门不能访问财务部。

网络拓扑

其网络拓扑图如图 5-14 所示。

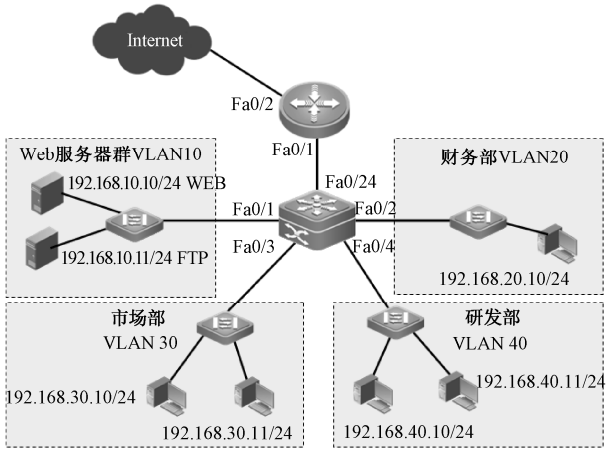


图 5-14　网络拓扑图

任务目标

实现部门间的访问安全，财务部不允许研发部访问，其他部门访问将被允许。

设备清单

三层交换机 1 台、二层交换机 4 台、路上器 1 台、PC N 台、线缆 N 条。

工作过程

标准访问列表对数据包过滤的依据是检查源 IP 地址和反子网掩码进行匹配，如果检查匹配正确将会触发拒绝（Deny）或者允许（Permit）动作。

对于任务一，首先对三层交换机进行基本配置，实现四个网段之间的互通。然后在三层

交换机创建标准访问控制列表，拒绝 192.168.40.0 网段（研发部）通过，允许其它网段通过。最后将创建好的策略应用在 Switch 三层交换机上的 F0/2 端口。配置步骤如下：

步骤一：进入特权，设置主机名。

步骤二：创建部门 VLAN。

步骤三：配置各部门 VLAN 的 IP 地址。

步骤四：将三层交换机的指定接口划入相应 VLAN。

步骤五：配置标准访问控制列表。

步骤六：将标准访问列表应用到接口。

具体配置如下：

步骤一：基本配置。

```
S>enable
S# configure terminal
S(config)#hostnaame Switch
```

步骤二：创建部门 VLAN。

```
Switch(config)#vlan 10
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#exit
Switch(config)#vlan 40
Switch(config-vlan)#exit
```

使用 show vlan 命令查看 VLAN，可以看到 4 个 VLAN 均已创建，如图 5-15 所示。

```
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Fa0/25, Fa0/26, Fa0/27, Fa0/28
                                                Fa0/29, Fa0/30, Fa0/31, Fa0/32
                                                Fa0/33, Fa0/34, Fa0/35, Fa0/36
                                                Fa0/37, Fa0/38, Fa0/39, Fa0/40
                                                Fa0/41, Fa0/42, Fa0/43, Fa0/44
                                                Fa0/45, Fa0/46, Fa0/47, Fa0/48
                                                Gi0/1, Gi0/2
10   VLAN0010                         active
20   VLAN0020                         active
30   VLAN0030                         active
40   VLAN0040                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

图 5-15　查看 VLAN

步骤三：配置各部门 VLAN 的 IP 地址。

```
Switch(config)#int vlan 10
Switch(config-VLAN 10)#ip address 192.168.10.1 255.255.255.0    //创建服务器群 IP
网段
Switch(config-VLAN 10)#exit
Switch(config)#int vlan 20
```

```
Switch(config-VLAN 20)#ip address192.168.20.1 255.255.255.0 //创建财务部 IP 网段
Switch(config-VLAN 20)#exit
Switch(config)#int vlan 30
Switch(config-VLAN 30)#ip address192.168.30.1 255.255.255.0 //创建市场部 IP 网段
Switch(config-VLAN 30)#exit
Switch(config)#int vlan 40
Switch(config-VLAN 40)#ip address192.168.40.1 255.255.255.0 //创建研发部 IP 网段
Switch(config-VLAN 40)#exit
```

步骤四：将三层交换机的指定接口划入相应 VLAN。

```
Switch(config)#int fastethernet 0/1
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#int fastethernet 0/2
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#int fastethernet 0/3
Switch(config-if)#switchport access vlan 30
Switch(config-if)#exit
Switch(config)#int fastethernet 0/4
Switch(config-if)#switchport access vlan 40
Switch(config-if)#exit
```

查看路由表，此时可以看到交换机的路由表中包含了 4 个网段的直连路由，如图 5-16 所示。

```
Switch(config)#show ip route
```

```
Switch#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.30.0/24 is directly connected, Vlan30
C    192.168.10.0/24 is directly connected, Vlan10
C    192.168.40.0/24 is directly connected, Vlan40
C    192.168.20.0/24 is directly connected, Vlan20
Switch#
```

图 5-16　查看路由表

步骤五：配置标准访问控制列表，如图 5-17 所示。

```
Switch(config)#access-list 1 deny 192.168.10.0 0.0.0.255
Switch(config)#access-list 1 deny 192.168.20.0 0.0.0.255
Switch(config)#access-list 1 permit 192.168.30.0 0.0.0.255
```

图 5-17　配置标准访问控制列表

拒绝来自研发部 192.168.40.0/24 网段的流量通过。

```
Switch(config)#access-list 1 deny 192.168.10.0 0.0.0.255
```

允许来自市场部 192.168.30.0/24 网段和服务器群 192.168.10.0/24 网段的流量通过。

```
Switch(config)#access-list 1 permit 192.168.30.0 0.0.0.255
Switch(config)#access-list 1 permit 192.168.10.0 0.0.0.255
```

步骤六：将访问控制列表应用在交换机 Switch 的 F0/2 端口的输出 out 方向。

```
Switch(config)#interface fastethernet 0/2
Switch(config-if)#ip access-group 1 out
Switch(config-if)#exit
```

项目测试

1．测试服务器和研发部主机到财务部主机的连通性，见表 5-5。

表 5-5 测试结果

序 号	源 IP 地址	目的 IP 地址	结 果	说 明
1	192.168.10.11	192.168.20.3	通	服务器群正常访问财务部主机
2	192.168.40.3	192.168.20.2	不通	研发部主机不能访问财务部主机

2．测试市场部主机到财务部主机的连通性，见表 5-6。

表 5-6 测试结果

序 号	源 IP 地址	目的 IP 地址	结 果	说 明
1	192.168.30.11	192.168.20.3	通	市场部主机能访问财务部主机

任务二 保护公司内部服务器访问安全

任务描述

你是该公司的网络管理员，公司服务器群分别架设 FTP、Web 服务器。其中 FTP 服务器供财务部专用，其他部门不可以使用；Web 服务器各部门均都可访问，FTP 及 Web 服务器、财务部、市场部和研发部分别属于不同的四个网段，四个网段之间通过三层交换机进行通信，要求你对三层交换机进行适当设置实现网络的数据流量控制。

网络拓扑

参考图 5-2。

任务目标

保护公司内部服务器访问安全，限制部门访问内容。

设备清单

三层交换机 1 台、二层交换机 4 台、路上器 1 台、PC N 台、线缆 N 条。

工作过程

扩展 ACL 可以控制源 IP、目的 IP、源端口、目的端口等，能实现相当精细的控制，扩展 ACL 不仅读取 IP 包头的源地址/目的地址，还要读取第四层包头中的源端口和目的端口的 IP。检查的元素中必须完全匹配才会触发拒绝（Deny）或允许（Permit）动作。

对于任务二，首先对三层交换机进行基本配置，实现四个网段可以互相访问；然后在三

层交换机上进行配置扩展访问列表，不允许 192.168.30.0 网段（市场部）和 192.168.40.0 网段（研发部）主机发送去往 192.168.10.0 网段的 FTP 数据包通过，允许 192.168.20.0 网段主机发送 FTP 和其他服务数据包通过，最后将这扩展访问列表应用到 Switch 的 F0/1 的输出 out 方向。

步骤一：进入特权模式，设置主机名。

步骤二：创建各部门 VLAN。

步骤三：配置各部门 VLAN 的 IP 地址。

步骤四：将三层交换机的指定接口划入相应 VLAN。

步骤五：配置扩展访问控制列表。

（1）允许财务部 192.168.20.0 网段访问服务器 IP 为 192.168.10.11 的 FTP 服务。

```
Switch(config)#access-list 100 permit tcp 192.168.20.0 0.0.0.255 host 192.168.10.11 eq ftp
```

（2）拒绝其它部门访问服务器 IP 为 192.168.10.11 的 FTP 服务。

```
Switch(config)#access-list 100 deny tcp any host 192.168.10.11 eq ftp
```

（3）允许所有部门主机访问服务器群的 WEB 服务。

```
Switch(config)#access-list 100 permit tcp any 192.168.10.0 0.0.0.255 eq 80
```

（4）允许其他服务的流量通过。

```
Switch(config)#access-list 100 permit ip any any
```

步骤六：将访问控制列表应用在交换机 Switch 的 F0/1 接口输出 OUT 方向。

```
Switch(config)#interface fastethernet 0/1
Switch(config-if)#ip access-group 100 out
Switch(config-if)#exit
```

项目测试

1．测试财务部主机能否使用 FTP 和 Web 服务，见表 5-7。

表 5-7　测试结果

序　号	源 IP 地址	目的 IP 地址	结　果	说　明
1	192.168.20.2	192.168.10.10	通	财务部主机可以访问 FTP 服务器
2	192.168.20.2	192.168.10.11	通	财务部主机可以访问 Web 服务器

2．测试市场部主机能否使用 FTP 和 Web 服务，见表 5-8。

表 5-8　测试结果

序　号	源 IP 地址	目的 IP 地址	结　果	说　明
1	192.168.30.2	192.168.10.11	不通	市场部主机不能访问 FTP 服务器
2	192.168.30.2	192.168.10.10	通	市场部主机可以访问 Web 服务器

3．测试研发部主机能否使用 FTP 和 Web 服务，见表 5-9。

表 5-9　测试结果

序　号	源 IP 地址	目的 IP 地址	结　果	说　明
1	192.168.40.2	192.168.10.11	不通	研发部主机不能访问 FTP 服务器
2	192.168.40.2	192.168.10.10	通	研发部主机可以访问 Web 服务器

任务三　控制员工上网时间

任务描述

你是该公司的网络管理员，为了保证公司员工上班期间的工作效率，公司上级要求上班时间员工只允许访问公司的内部网站。而下班后员工可以随意访问网络不受限制。

网络拓扑

参考图 5-2。

任务目标

保证公司员工上班时间的工作效率，控制员工上网时间及访问内容。

设备清单

三层交换机 1 台、二层交换机 4 台、路上器 1 台、PC N 台、线缆 N 条。

工作过程

基于时间的访问控制列表使管理员可以依据时间来控制用户对网络资源的访问，可以根据时间来允许/拒绝用户访问通信。实现时间的 ACL 功能，必须先创建一个 Time-range 接口来指定时间与日期。然后再将 Time-range 接口与对应的 ACL 关联起来。

对于这一工作任务，首先在交换机上进行基本配置，然后创建基于时间的访问控制列表，将这个时间的访问控制列表应用在交换机上的 F0/24 端口的出方向 out。

步骤一：进入特权，设置主机名

步骤二：创建部门 VLAN

步骤三：配置各部门 VLAN 的 IP 地址

步骤四：将三层交换机的指定接口划入相应 VLAN

步骤五：配置交换机的时钟

```
Switch#show clock
00:00:09 bj Sun, Aug 18, 1994
```

调整交换机当前时钟和实际时钟同步

```
Switch#clock set 20:36:10 3 oct 2013
```

步骤六：定义时间段

```
Switch(config)# time-range freetime
Switch(config-time-range)#periodic daily 0:00 to 9:00
Switch(config-time-range)#periodic daily 17:00 to 23:59
```

步骤七：配置命名时间访问控制列表

```
Switch(config)#ip access-list extended timeacl
```

（1）允许服务器群任何时间都可以访问网络

```
Switch(config-ext-nacl)# permit ip 192.168.10.0 0.0.0.255 any
```

（2）允许财务部只能在规定时间访问网络

```
Switch(config-ext-nacl)#permit ip 192.168.20.0 0.0.0.255 any time-range freetime
```

（3）允许市场部只能在规定时间访问网络

```
Switch(config-ext-nacl)# permit ip 192.168.30.0 0.0.0.255 any time-range freetime
```

（4）允许研发部只能在规定时间访问网络

```
Switch(config-ext-nacl)# permit ip 192.168.40.0 0.0.0.255 any time-range freetime
```

（5）其它时间将拒绝访问

```
Switch(config-ext-nacl)#deny ip any any
```

步骤八：将时间访问控制列表应用在交换机 Switch 的 F0/24 接口输出 OUT 方向。

```
Switch(config)#interface fastethernet 0/24
Switch(config-if)#ip access-group timerange out
Switch(config-if)#exit
```

项目测试

1．验证在工作时间内的访问。

更改交换机的当前时间为上班时间，财务部、市场部、研发部将只可以访问公司 Web 服务。测试结果见表 5-10。

表 5-10　测试结果

序　　号	源 IP 地址	目的 IP 地址	结　　果	说　　明
1	192.168.20.2	外网	不通	工作时间不能访问外网
2	192.168.30.2	外网	不通	工作时间不能访问外网
3	192.168.40.2	外网	不通	工作时间不能访问外网

2．验证在非工作时间内的访问

更改交换机的当前时间为下班时间，财务部、市场部、研发部将可以随意访问。测试结果见表 5-11。

表 5-11　测试结果

序　　号	源 IP 地址	目的 IP 地址	结　　果	说　　明
1	192.168.20.2	外网	通	工作时间可以访问外网
2	192.168.30.2	外网	通	工作时间可以访问外网
3	192.168.40.2	外网	通	工作时间可以访问外网

3．服务器群在任何时间都可以随便访问外部网络。测试结果见表 5-12。

表 5-12　测试结果

序　　号	源 IP 地址	目的 IP 地址	结　　果	说　　明
1	192.168.10.10	外网	通	任何时间可以访问外网
2	192.168.10.11	外网	通	任何时间可以访问外网

认证测试

一、选择题

1．标准访问控制列表的数字标识范围是（　　）。

A．1～50　　B．1～99　　C．1～100　　D．1～199

2．使配置的访问列表应用到接口上的命令是什么（　　）。

A．access-group　B．access-list　　C．ip access-list　　D．ip access-group

3．下面关于访问控制列表的配置命令，正确的是（　　）。

A．access-list 100 deny 1.1.1.1

B．access-list 1 permit any

C．access-list 1 permit 1.1.1.1 0 2.2.2.2 0.0.0.255

D．access-list 99 deny tcp any 2.2.2.2 0.0.0.2554

4．IP 扩展访问列表的数字标示范围是（　　）。

A．0～99　　B．1～99　　C．100～199　　D．101～200

5．IP 标准访问控制列表是基于下列哪一项来允许和拒绝数据包的（　　）。

A．TCP 端口号　B．UDP 端口号　　C．ICMP 报文　　D．源 IP 地址

二、简答题

1．标准访问控制列表和扩展访问控制列表的区别在哪里？

2．使用访问控制列表能够带来什么好处？

3．简述配置时间访问控制列表的命令过程？

4．简述配置扩展访问控制列表实现 Web 访问限制的命令过程？

项目六　新锐集团公司网络配置与管理

项目背景

新锐集团公司总部设在北京市，由于业务发展的需要，已在上海和广州分别设置了分公司，为了实现快捷的信息交流和资源共享，需要构建一个跨越三地的集团网络，要求网络具有良好的稳定性和较高的安全性，并且还要具有较好的扩展性和可管理性。总公司有研发部、营销部、市场部和管理部四个部门，上海分公司设有销售一部和销售二部，广州分公司设有销售三部，由于业务的迅速发展，人员增加到 50 多人，于是增设了销售四部。北京总公司现有网络拓扑如图 6-1 所示，上海分公司和广州分公司网络拓扑如图 6-2 和图 6-3 所示。

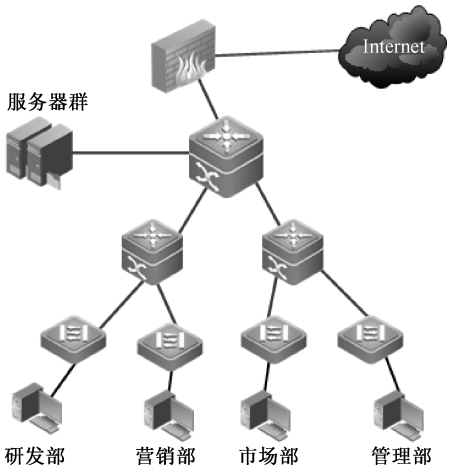


图 6-1　北京总公司网络拓扑图

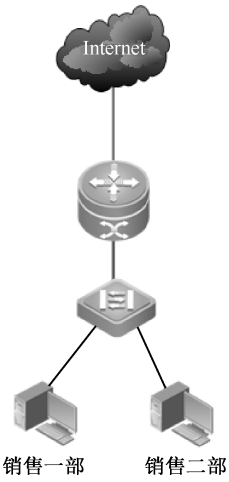


图 6-2　上海分公司网络拓朴图

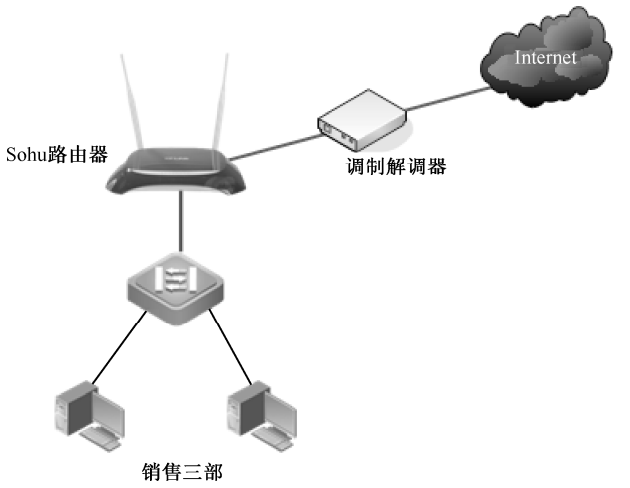


图 6-3　广州分公司网络拓扑图

项目分析

要实现跨越三地的集团网络，可以通过 VPN（虚拟专用网络）或者租用专线来解决，租用专线构建的网络比采用 VPN 技术构建的网络更稳定和安全。

为了适应今后网络的扩展和方便管理，应采用动态路由技术实现三地网络的互联互通。

由于广州分公司业务的迅速发展，人员增加到 50 多人，原来的 sohu 路由器不能满足上网需求和与总公司网络互联的要求,网络需要升级改造。

项目方案

由于集团公司要求网络要具有较高的稳定性和安全性，所以采用租用专线的方案实现总公司与分公司之间的网络连通。北京总公司通过增加一台路由器与分公司之间进行互联。上海分公司已有路由器，只需将专线接入路由器即可与总公司连通。为了满足广州分公司的上网需求和总公司网络互联的要求，需将现有的 ADSL 接入改造为光纤接入。集团公司的网络拓扑如图 6-4 所示。

要想实现总公司与分公司间的数据通信，还需要在路由器上配置路由。采用静态路由，网络发生变化时，由于网络模型比较大，网络管理员手动配置路由需要花较多的时间,而且还容易出现配置不当而带来网络故障。这样不能快速地使网络畅通,同时增加管理员的管理负担，不能满足公司对网络管理和使用的要求。采用动态路由协议，总公司与分公司的网络可以实现动态自动学习网络间的路由信息，从而实现网络间的畅通。所以决定在集团公司网络中使用 OSPF 动态路由协议。

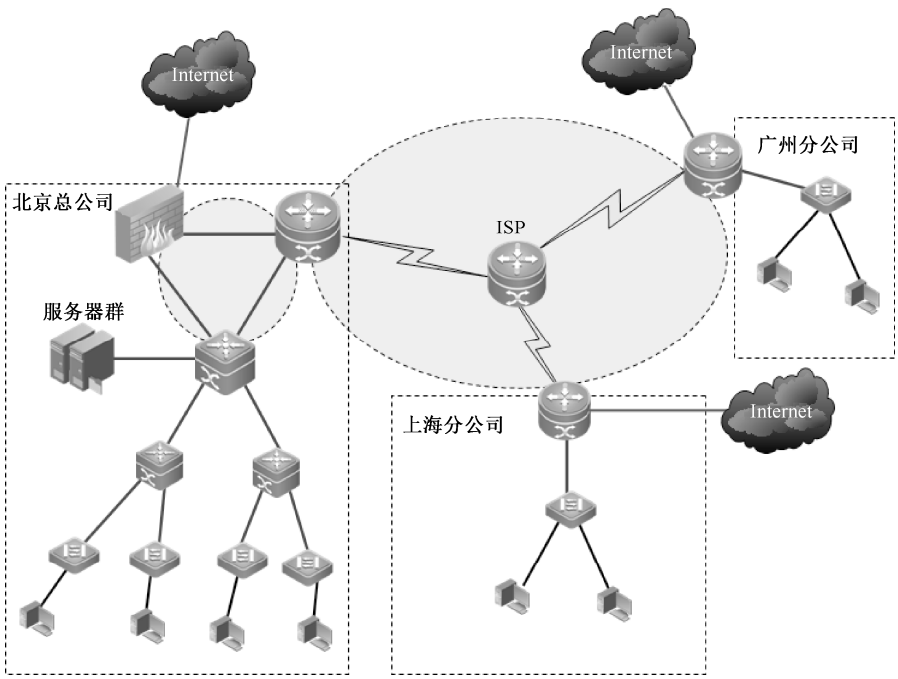


图 6-4　网络拓扑图

知识准备

1．动态路由协议概述

1）动态路由协议概念

动态路由是指利用路由器上运行的动态路由协议定期和其他路由器交换路由信息，而从

其他路由器上学习到的路由信息，自动建立起自己的路由。根据是否在一个自治域内部使用，动态路由协议分为内部网关协议（IGP）和外部网关协议（EGP）。这里的自治域指一个具有统一管理机构、统一路由策略的网络。自治域内部采用的路由选择协议称为内部网关协议，常用的有 RIP、OSPF；外部网关协议主要用于多个自治域之间的路由选择，常用的是 BGP 和 BGP-4。

2．动态路由协议种类

（1）距离矢量路由协议

计算网络中链路的距离矢量，然后根据计算结果进行路由选择。路由器定期向邻居路由器发送消息，消息的内容就是自己的整个路由表，如：到达目的网络所经过的距离；到达目的网络的下一跳地址运行距离矢量的路由器会根据相邻路由器发送过来的信息，更改自己的路由表。

距离矢量名称的由来是因为路由是以矢量（距离，方向）的方式被通告出去的，这里的距离是根据度量来决定的。通俗点就是：往某个方向上的距离。

每种路由协议都有自己的算法，路由协议在共享和传递路由更新信息，乃至收敛都因为算法的不同而不同。

每台路由器在信息上都依赖于自己的相邻路由器，而它的相邻路由器又是通过自它们自己的相邻路由器那里学习路由，依此类推，所以就好象街边巷尾的小道新闻——一传十，十传百，很快就能弄到家喻户晓了。呵呵。正因为如此，我们一般把距离矢量路由协议称之为“依照传闻的路由协议”

路由以矢量（距离、方向）的方式被通告出去的，其中距离是根据度量来定义的，方向是根据下一跳路由器定义的。被认为是“依照传闻进行路由选择”。

协议特点：

距离矢量协议直接传送各自的路由表信息。网络中的路由器从自己的邻居路由器得到路由信息，并将这些路由信息连同自己的本地路由信息发送给其他邻居，这样一级级的传递下去以达到全网同步。每个路由器都不了解整个网络拓扑，它们只知道与自己直接相连的网络情况，并根据从邻居得到的路由信息更新自己的路由表。距离矢量协议无论是实现还是管理都比较简单，但是它的收敛速度慢，报文量大，占用较多网络开销，并且为避免路由环路得做各种特殊处理。目前基于距离矢量算法的协议包括 RIP、IGRP、EIGRP、BGP。其中 BGP 是距离矢量协议变种，它是一种路径矢量协议。

典型的距离向量路由选择协议有：

RIP 协议

RIP（Routing Information Protocols，路由信息协议）是使用最广泛的距离矢量协议，它是由施乐（Xerox）在 70 年代开发的。TCP/IP 版本的 RIP 是施乐协议的改进版。RIP 最大的特点是，无论实现原理还是配置方法，都非常简单。RIP 基于跳数计算路由，并且定期向邻居路由器发送更新消息。

IGRP 协议

IGRP 是 CISCO 专有的协议，只在 CISCO 路由器中实现。它也属于距离矢量类协议，所以在很多地方与 RIP 有共同点，比如广播更新等等。它和 RIP 最大的区别表现在度量方法、负载均衡等几方面。IGRP 支持多路径上的加权负载均衡，这样网络的带宽可以得到更加合理的利用。另外，与 RIP 仅使用跳数作为度量依据不同，IGRP 使用了多种参数，构成复合的度

量值，这其中可以包含的因素有：带宽、延迟、负载、可靠性和 MTU（最大传输单元）等等。

EIGRP 协议

EIGRP 是 IGRP 的增强版，它也是 CISCO 专有的路由协议。EIGRP 采用了扩散更新（DUAL）算法，在某种程度上，它和距离向量算法相似，但具有更短的收敛时间和更好的可操作性。作为对 IGRP 的扩展，EIGRP 支持多种可路由的协议，如 IP、IPX 和 AppleTalk 等等。运行在 IP 环境时，EIGRP 还可以与 IGRP 进行平滑的连接，因为它们的度量方法是一致的。

（2）链路状态路由协议

链路状态路由选择协议的目的是得到整个网络的拓扑结构。运行链路状态路由协议的每个路由器都要提供链路状态的拓扑结构信息，信息的内容包括：路由器所连接的网段链路；以及该链路的物理状态。根据返回的信息，路由器根据网络拓扑结构的变化及时修改路由配置，以适应新的路由选择。

链路状态路由选择协议又称为最短路径优先协议，它基于 Edsger Dijkstra 的最短路径优先（SPF）算法。它比距离矢量路由协议复杂得多，但基本功能和配置却很简单，甚至算法也容易理解。路由器的链路状态的信息称为链路状态，包括：接口的 IP 地址和子网掩码、网络类型（如以太网链路或串行点对点链路）、该链路的开销、该链路上的所有的相邻路由器。

典型的链路状态路由选择协议有：

最短路径优先（OSPF）

OSPF 由 IETF 的 OSPF 工作组设计，OSPF 的开发始于 1987 年，如今正在使用的有 OSPFv2 和 OSPFv3 两个版本。OSPF 的大部分工作由 John Moy 完成。

中间系统到中间系统（IS-IS）

IS-IS 由 ISO 设计的，它的雏形由 DEC 开发，名为 DECnet Phase V，首席设计师是 Radia Perlman.IS-IS 最初是为 OSI 协议簇而非 TCP/IP 协议簇而设计的，后来，集成化 IS-IS，即双 IS-IS 添加了对 IP 网络的支持，尽管 IS-IS 路由协议一直主要供 ISP 和电信公司使用，但已有越来越多的企业开始使用 IS-IS。

3．RIP 动态路由协议

1）RIP 协议概述

RIP（Routing Information Protocols，路由信息协议），是应用较早、使用较普遍的内部网关协议（Interior Gateway Protocol，IGP），适用于小型同类网络，是典型的距离矢量（distance-vector）协议。

RIP 协议最初是为 Xerox 网络系统的 Xerox parc 通用协议而设计的，是 Internet 中常用的路由协议。RIP 采用距离向量算法，即路由器根据距离选择路由，所以也称为距离向量协议。路由器收集所有可到达目的地的不同路径，并且保存有关到达每个目的地的最少站点数的路径信息，除到达目的地的最佳路径外，任何其它信息均予以丢弃。同时路由器也把所收集的路由信息用 RIP 协议通知相邻的其它路由器。这样，正确的路由信息逐渐扩散到了全网。

RIP 使用非常广泛，它简单、可靠，便于配置。但是 RIP 只适用于小型的同构网络，因为它允许的最大站点数为 15，任何超过 15 个站点的目的地均被标记为不可达。而且 RIP 每隔 30s 一次的路由信息广播也是造成网络的广播风暴的重要原因之一。

RIP 是基于 UDP，端口 520 的应用层协议。RIP 协议每隔 30 秒向外发送一次更新报文。如果设备经过 180 秒没有收到来自对端的路由更新报文则将所有来自此设备的路由信息标志为不可达，若在 240 秒内仍未收到更新报文就将这些路由从路由表中删除。

2）RIP 协议的路由算法

RIP 协议使用跳数来衡量到达目的地的距离，称为网络的度量值（metric）。在 RIP 协议中，设备到与它直接相连网络的跳数为 0；通过一个设备可达的网络的跳数为 1，其余依此类推；如果从网络的一个终端到另一个终端的路由跳数超过 15 个，将被认为是可不到达的。

3）RIP 协议的版本

RIP 协议有 RIPv1 和 RIPv2 两个版本，两者区别如下表所示：

	RIPv1	RIPv2
路由协议	有类	无类
VLSM	不支持	支持
报文更新方式	广播	组播
认证方式	不支持	支持明文和 MD5 认证
手工汇总	不支持	在关闭自动汇总后可进行手工汇总

4）配置 RIP 协议

RIP 协议配置如图 6-5 所示。

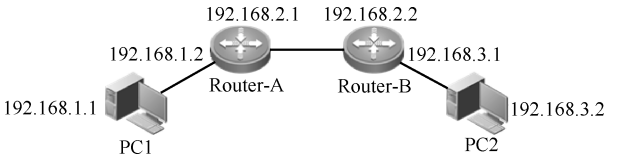


图 6-5　RIP 配置实例

（1）配置步骤

第 1 步：开启 RIP 路由协议进程：

```
Router(config)# router rip
```

第 2 步：宣告路由器 A 和路由器 B 参与 RIP 协议的网段信息：

```
Router-A(config-router)# network 192.168.1.0
Router-A(config-router)# network 192.168.2.0
Router-B(config-router)# network 192.168.2.0
Router-B(config-router)# network 192.168.3.0
```

第 3 步：指定 RIP 协议的版本 2（默认是 version1）：

```
Router(config-router)# version  2
```

第 4 步：在 RIPv2 版本中关闭自动汇总：

```
Router(config-router)# no auto-summary
```

（2）查看 RIP 配置信息

- 验证 RIP 的配置：

```
Router# show ip protocols
```

- 显示路由表的信息：

```
Router# show ip route
```

- 清除 IP 路由表的信息：

```
Router# clear ip route
```

- 在控制台显示 RIP 的工作状态：

```
Router# debug ip rip
```

4．OSPF 动态路由协议

1）OSPF 协议概述

OSPF（Open Shortest Path First，开放式最短路径优先）为 IETF OSPF 工作组开发的一种基于链路状态的内部网关路由协议。OSPF 协议是专为 IP 开发的路由协议，直接运行在 IP 层上面，协议号为 89，采用组播方式进行 OSPF 包交换，组播地址为 224.0.0.5（全部 OSPF 路由器）和 224.0.0.6（指定路由器）。

80 年代中期，RIP 已不能适应大规模异构网络的互连，0SPF 随之产生。它是网间工程任务组织（IETF）的内部网关协议工作组为 IP 网络而开发的一种路由协议。

OSPF 是一种基于链路状态的路由协议，需要每个路由器向其同一管理域的所有其它路由器发送链路状态广播信息。在 OSPF 的链路状态广播中包括所有接口信息、所有的量度和其它一些变量。利用 OSPF 的路由器首先必须收集有关的链路状态信息，并根据一定的算法计算出到每个节点的最短路径。而基于距离向量的路由协议仅向其邻接路由器发送有关路由更新信息。

与 RIP 不同，OSPF 将一个自治域再划分为区，相应地即有两种类型的路由选择方式：当源和目的地在同一区时，采用区内路由选择；当源和目的地在不同区时，则采用区间路由选择。这就大大减少了网络开销，并增加了网络的稳定性。当一个区内的路由器出了故障时并不影响自治域内其它区路由器的正常工作，这也给网络的管理、维护带来方便。

与 RIP 路由协议对比，OSPF 协议除了算法上的不同，还引入了路由更新认证、VLSMs（可变长子网掩码）、路由聚合等新概念。即使 RIPv2 做了很大的改善，可以支持路由更新认证、可变长子网掩码等特性，但是 RIP 协议还是存在两个致命弱点：

（1）收敛速度慢；

（2）网络规模受限制，最大跳数不超过 15 跳。

OSPF 协议的出现克服了 RIP 协议的弱点，可以胜任中大型、较复杂的网络环境。

2）OSPF 协议的路由算法

OSPF 路由协议使用基于 Dijkstra 提出的最短路径优先算法（SPF）计算路由。同时，它是一个开发的协议。

3）OSPF 协议的版本

OSPFv1　测试版本，仅在实验平台使用。

OSPFv2　发行版本，目前使用的都是这个版本。

OSPFv3　测试版本，提供对 IPv6 的路由支持。

4）OSPF 协议的相关术语

（1）路由器 ID（Router ID）

OSPF 技术使用路由器 ID 号来唯一标识网络中每一台路由器。它是一个 32 位无符号整数，和 IP 地址长度相同。路由器 ID 可以手工配置，如果为进行手工配置，则路由器就在其端口所配置的 IP 地址中，选出一个地址作为路由器 ID。

选择顺序为：首先在当前路由器的所有 Lookback 端口中选择 IP 地址最大的作为本路由器的 ID；如果当前路由器没有配置 Lookback 端口地址，就从其他端口的 IP 地址中选择最大的作为本路由器的 ID。

（2）自治系统（Autonamous System）

一个自治系统就是处于一个管理机构控制之下的路由器和网络群组。它可以是一个路由器直接连接到一个 LAN 上，同时也连到 Internet 上；它可以是一个由企业骨干网互连的多个局域网。在一个自治系统中的所有路由器必须相互连接，运行相同的路由协议，同时分配同一个自治系统编号。

（3）区域（Area）

路由协议传递消息需要占用网络带宽，网络规模越大，其占用网络带宽就越大。解决问题的办法就是要缩小消息传递的范围，将可以接受的链路状态传递流量限制在合理的范围，这个范围就是区域（Area）。OSPF 区域将网络分为若干和较小部分，以减少每台路由器存储和维护的信息量。

一个区域用 32 位无符号数字标识。区域 0 被保留，用来标识骨干网络，一个 OSPF 网络必须有一个骨干区域。其他所有区域必须直接连接在区域 0 上，这是避免区域间形成路由环路的关键因素。

（4）骨干区域（Backbone Area）

OSPF 划分区域之后，并非所有的区域都是平等的关系。其中有一个区域是与众不同的，它的区域号（Area ID）是 0，通常被称为骨干区域。骨干区域负责区域之间的路由，非骨干区域之间的路由信息必须通过骨干区域来转发。对此，OSPF 有两个规定：1，所有非骨干区域必须与骨干区域保持连通；2，骨干区域自身也必须保持连通。但在实际应用中，可能会因为各方面条件的限制，无法满足这个要求。这时可以通过配置 OSPF 虚连接（Virtual Link）予以解决。

（5）虚连接（Virtual Link）

虚连接是指在两台 ABR 之间通过一个非骨干区域而建立的一条逻辑上的连接通道。它的两端必须是 ABR，而且必须在两端同时配置方可生效。为虚连接两端提供一条非骨干区域内部路由的区域称为传输区（Transit Area）。

（6）区域边界路由器 ABR（Area Border Router）

该类路由器可以同时属于两个以上的区域，但其中一个必须是骨干区域。ABR 用来连接骨干区域和非骨干区域，它与骨干区域之间既可以是物理连接，也可以是逻辑上的连接。

5）配置 OSPF 协议

配置单区域 OSPF，如图 6-6 所示。

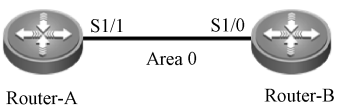


图 6-6　单区域 OSPF

配置步骤如下。

```
ROUTER-A                                    ROUTER-B
S1/1    192.168.1.1/24                          S1/0        192.168.1.2/24
Loopback0  10.10.10.1/24                        Loopback0   10.10.11.1/24
```

第 1 步：路由器环回接口的配置（其他接口配置请参见前面所学课程）

路由器 A：

```
Router-A#interface  loopback0                    //设置 loop 口
Router-A(config)#ip address 10.10.10.1 255.255.255.0
```

路由器 B：

```
Router-B#config
Router-B(config)#interface loopback0
Router-B(config)#ip address  10.10.11.1 255.255.255.0
```

第 2 步：验证接口配置。

```
Router-B#sh interface loopback0
Loopback0 is up, line protocol is up
Hardware is Loopback
Interface address is 10.10.11.1/24
MTU 1514 bytes, BW 8000000 kbit, DLY 500 usec
Encapsulation LOOPBACK
```

第 3 步：路由器的 OSPF 配置。

```
Router-A 的配置：
Router-A(config)#router ospf 1          //启动 OSPF 进程，进程号为 1
Router-A(config)_ospf_1#network 10.10.10.0 0.0.0.255 area 0
//注意要写反掩码（通配符）和区域号
Router-A(config)_ospf_1#network 192.168.1.0 0.0.0.255 area 0
Router-B 的配置：
Router-B(config)#router ospf 1
Router-B(config)_ospf_1#network 10.10.11.0 0.0.0.255 area 0
Router-B(config)_ospf_1#network 192.168.1.0 0.0.0.255 area 0
```

第 4 步：查看路由表。

```
Router-A#sh ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - DEIGRP, DEX - external DEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type
VRF ID: 0
C     10.10.10.0/24       is directly connected, Loopback0
O     10.10.11.0/24       [110,1600] via 192.168.1.2(on Serial1/1)
                    //注意到环回接口产生的是主机路由
C     192.168.1.0/24      is directly connected, Serial1/1
Router-B#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - DEIGRP, DEX - external DEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type
```

```
VRF ID: 0
O     10.10.10.0/24     [110,1601] via 192.168.1.1(on Serial1/0)
//注意管理距离为 110
C     10.10.11.0/24       is directly connected, Loopback0
C     192.168.1.0/24      is directly connected, Serial1/0
```

第 5 步：其他验证命令。

```
Router-B#sh ip ospf 1                    //显示该 OSPF 进程的信息
OSPF process: 1, Router ID: 192.168.2.1
Distance: intra-area 110,  inter-area 110,  external 150
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
SPFTV:11(1), TOs:24, SCHDs:27
All Rtrs support Demand-Circuit.
Number of areas is 1
AREA: 0
  Number of interface in this area is 2(UP: 3)
  Area authentication type:  None
  All Rtrs in this area support Demand-Circuit.
Router-A#show ip ospf interace          //显示 OSPF 接口状态和类型
Serial1/1 is up, line protocol is up
  Internet Address: 192.168.1.1/24
  Nettype: Point-to-Point
  OSPF process is 2,  AREA: 0, Router ID: 192.168.1.1
  Cost: 1600, Transmit Delay is 1 sec, Priority 1
  Hello interval is 10, Dead timer is 40, Retransmit is 5
  OSPF INTF State is IPOINT_TO_POINT
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.1.2
Loopback0 is up, line protocol is up
  Internet Address: 10.10.10.1/24
  Nettype: Broadcast                //环回接口的网络类型默认为广播
  OSPF process is 2,  AREA: 0, Router ID: 192.168.1.1
  Cost: 1, Transmit Delay is 1 sec, Priority 1
  Hello interval is 10, Dead timer is 40, Retransmit is 5
  OSPF INTF State is ILOOPBACK
  Neighbor Count is 0, Adjacent neighbor count is 0
Router-A#sh ip ospf neighbor                    //显示 OSPF 邻居
-------------------------------------------------------------------
                          OSPF process: 2
                           AREA: 0
Neighbor ID     Pri   State       DeadTime   Neighbor Addr   Interface
192.168.2.1     1     FULL/-      31         192.168.1.2     Serial1/1
Router-A#sh ip ospf interface
Serial1/1 is up, line protocol is up
  Internet Address: 192.168.1.1/24
```

```
  Nettype: Point-to-Point
  OSPF process is 2,  AREA: 0, Router ID: 192.168.1.1
  Cost: 1600, Transmit Delay is 1 sec, Priority 1
  Hello interval is 10, Dead timer is 40, Retransmit is 5
  OSPF INTF State is IPOINT_TO_POINT
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.1.2
Loopback0 is up, line protocol is up
  Internet Address: 10.10.10.1/24
  Nettype: Point-to-Point
  OSPF process is 2,  AREA: 0, Router ID: 192.168.1.1
  Cost: 1, Transmit Delay is 1 sec, Priority 1
  Hello interval is 10, Dead timer is 40, Retransmit is 5
  OSPF INTF State is IPOINT_TO_POINT
  Neighbor Count is 0, Adjacent neighbor count is 0
```

配置多区域 OSPF，如图 6-7 所示。

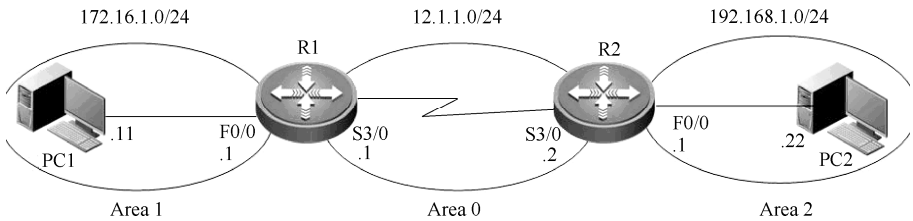


图 6-7　多区域 OSPF

配置步骤如下。

第 1 步：配置各台路由器用户名和接口 IP 地址，并且使用 ping 命令确认各路由器的直连口的互通性。

```
R1#ping 12.1.1.2
Sending 5, 100-byte ICMP Echoes to 12.1.1.2, timeout is 2 seconds:
< press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R1#ping 172.16.1.11
Sending 5, 100-byte ICMP Echoes to 172.16.1.11, timeout is 2 seconds:
< press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R1#show ip rou
Codes:  C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
ia - IS-IS inter area, * - candidate default
Gateway of last resort is no set
C   12.1.1.0/24 is directly connected, Serial 3/0
C   12.1.1.1/32 is local host.
C   172.16.1.0/24 is directly connected, FastEthernet 0/0
C   172.16.1.1/32 is local host.
```

第 2 步：在 R1 上启动 OSPF 路由协议。

```
R1(config)#router ospf 100              //启动 OSPF 进程，进程号为 100
R1(config-router)#router-id 1.1.1.1     //设置 R1 的 ID，router-id 相当于 loopback0，
都是一种路由器的标识 ID。
Change router-id and update OSPF process! [yes/no]:yes
R1(config-router)#network 12.1.1.0 0.0.0.255 area 0          //配置骨干区域 0
R1(config-router)#network 172.16.1.0 0.0.0.255 area 1        //配置分支区域 1
R1(config-router)#end
```

第 3 步：在 R2 上启动 OSPF 路由协议。

```
R2(config)#router ospf 100
R2(config-router)#router-id 2.2.2.2
Change router-id and update OSPF process! [yes/no]:yes
R2(config-router)#network 12.1.1.0 0.0.0.255 area 0
R2(config-router)#network 192.168.1.0 0.0.0.255 area 2
```

第 4 步：验证测试：（以 R1 为例）。

```
R1#show ip route
Codes:  C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default
Gateway of last resort is no set
C   12.1.1.0/24 is directly connected, Serial 3/0
C   12.1.1.1/32 is local host.
C   172.16.1.0/24 is directly connected, FastEthernet 0/0
C   172.16.1.1/32 is local host.
O IA 192.168.1.0/24 [110/51] via 12.1.1.2, 00:01:02, Serial 3/0
//可以看出 R1 学到了 Area 2 里面的路由条目，其中 IA 代表区域间的路由
R1#show ip ospf database
//查看 ospf 的链路状态数据库，因为 R1 即属于 Area1，有属于 Area0，所以 R1 有两个链路状态数据库
OSPF Router with ID (1.1.1.1) (Process ID 100)
Router Link States (Area 0.0.0.0)
Link ID    ADV Router      Age     Seq     CkSum       Link count
1.1.1.1    1.1.1.1         73      0x80000003 0x367a 2
2.2.2.2    2.2.2.2         69      0x80000003 0xd5d5 2
Summary Link States (Area 0.0.0.0)
Link ID    ADV Router      Age  Seq#       CkSum  Route
172.16.1.0 1.1.1.1         143             0x80000001 0xc6d3 172.16.1.0/24
```

```
192.168.1.02.2.2.2          75              0x80000001 0x7c6d 192.168.1.0/24
Router Link States (Area 0.0.0.1)
Link ID     ADV Router      Age     Seq#        CkSum       Link count
1.1.1.1     1.1.1.1         103             0x80000003 0xd1b7 1
Summary Link States (Area 0.0.0.1)
Link ID     ADV Router      Age     Seq#        CkSum       Route
12.1.1.0        1.1.1.1         143             0x80000001 0x8f89
12.1.1.0/24
192.168.1.01.1.1.1          68              0x80000001 0x902b   192.168.1.0/24
R1#show ip ospf neighbor //查看 R1 的 ospf 邻居，处于 Full 状态
OSPF process 100, 1 Neighbors, 1 is Full:
Neighbor ID     Pri     State           Dead Time       Address     Interface
2.2.2.2         1       Full/-      00:00:32        12.1.1.2        Serial 3/0

R1#ping 192.168.1.22                            //在 R1 上 ping PC2
Sending 5, 100-byte ICMP Echoes to 192.168.1.22, timeout is 2 seconds:
< press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 30/32/40 ms
//在 PC1 上 ping PC2
```

第 5 步：试验完成。

在 PC1 上通过 ping 命令测试到 PC2 的连通性。测试连通性如图 6-8 所示。

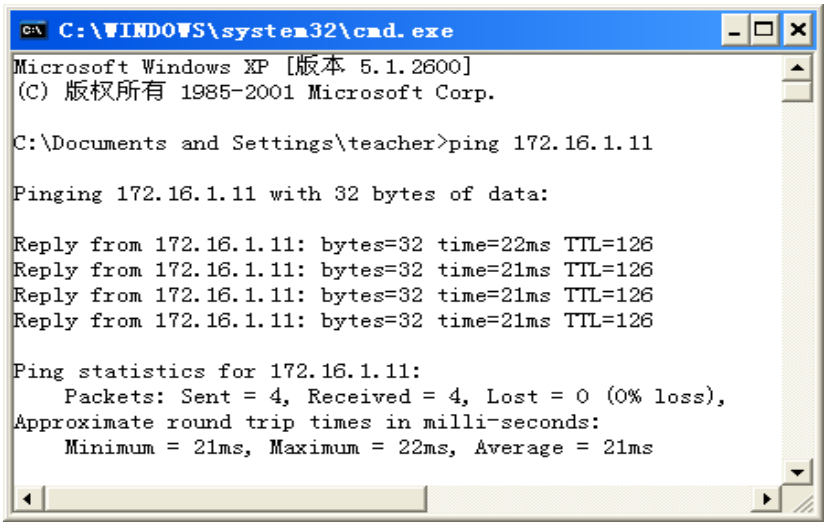


图 6-8　测试连通性

5．NAT 技术

1）NAT 概述

网络地址转换（Network Address Translation，NAT）属接入广域网（WAN）技术，是一种将私有的 IP 地址转化为合法公有 IP 地址的转换技术，它被广泛应用于各种类型 Internet 接入方式和各种类型的网络中。

NAT 的典型应用是将使用私有 IP 地址的网络连接到 Internet，这样公司就无需再给内部网络中的每个设备都分配公有 IP 地址，既节省了申请公有 IP 的费用，又避免了公有地址的浪费，有效缓解了 IPv4 地址不足的问题。另一方面，通过地址转换，可以隐藏内网上主机的真实 IP 地址，从而提高网络的安全性。

2）NAT 术语（图 6-9）

内部/外部：IP 主机相对于 NAT 设备的物理位置。

本地/全局：用户相对于 NAT 设备的位置或视角。

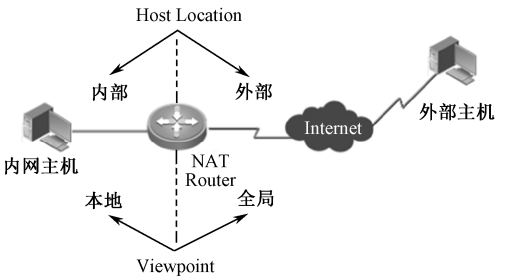


图 6-9　NAT 术语

内部本地地址：分配给内部网络中的主机的 IP 地址，通常是私有地址。

内部全局地址：合法的公有 IP 地址，通常由 ISP 提供，全局唯一的。

外部全局地址：外部网络中的主机 IP 地址，来自全局可路由的地址空间。

外部本地地址：在内部网络中看到的外部主机的 IP 地址，通常是私有地址。

3）NAT 的三种实现方式

（1）静态 NAT

指将内部网络的私有 IP 地址转换为公有 IP 地址时，IP 地址对是一对一的，是一成不变的，某个私有 IP 地址只转换为某个公有 IP 地址。私有地址和公有地址的对应关系由管理员手工指定。这种方式经常用于企业网的内部服务器能够被外部网络访问时。

（2）动态 NAT

指将内部网络的私有 IP 地址转换为公用 IP 地址时，IP 地址对并不是一一对应的，而是随机的。所有被管理员授权访问外网的私有 IP 地址可随机转换为任何指定的公有 IP 地址。也就是说，只要指定哪些内部地址可以进行转换，以及用哪些合法地址作为外部地址（建立地址池）时，就可以进行动态转换。每个地址的租用时间都有限制。这样，当 ISP 提供的合法 IP 地址略少于网络内部的计算机数量时，可以采用动态转换的方式。内部地址可以使用地址池中的外部地址。多个内部地址共享几个外部地址。

（3）端口多路复用 PAT（Port address Translation)

通过使用端口多路复用，可以达到一个公网地址对应多个私有地址的一对多转换。在这种工作方式下，内部网络的所有主机均可共享一个合法外部 IP 地址实现对 Internet 的访问，来自不同内部主机的流量用不同的随机端口进行标示，从而可以最大限度地节约 IP 地址资源。同时，又可隐藏网络内部的所有主机，有效避免来自 internet 的攻击。因此，目前网络中应用最多的就是端口多路复用方式。

4）配置 NAT

（1）配置静态 NAT（见图 6-10）

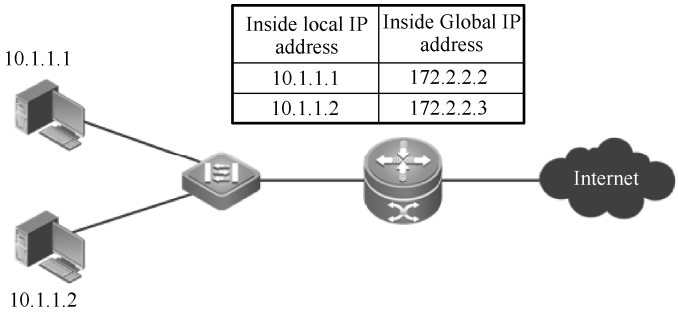


图 6-10 静态 NAT

第 1 步：定义内网接口和外网接口。

```
Router(config)# interface fastethernet 1/0
Router(config-if)# ip nat outside
Router(config)# interface fastethernet 1/1
Router(config-if)# ip nat inside
```

第 2 步：建立静态的映射关系。

```
Router(config)# ip nat inside source static 10.1.1.1 172.2.2.2
Router(config)# ip nat inside source static 10.1.1.2 172.2.2.3
```

（2）配置动态 NAT（见图 6-11）

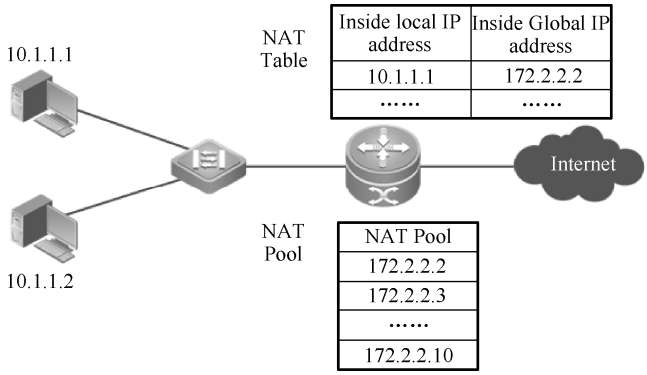


图 6-11 动态 NAT

第 1 步：定义内网接口和外网接口。

```
Router(config-if)# ip nat outside
Router(config-if)# ip nat inside
```

第 2 步：定义内部本地地址范围。

```
Router(config)# access-list 10 permit 10.1.1.0 0.0.0.255
```

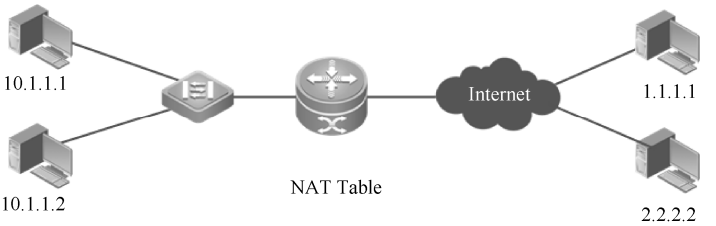
第 3 步：定义内部全局地址池。

```
Router(config)#ip nat pool abc 172.2.2.2 172.2.2.2 netmask 255.255.255.0
```

第 4 步：建立映射关系。

```
Router(config)# ip nat inside source list 10 pool abc
```

（3）配置动态 PAT（见图 6-12）



Protocol	Inside Local IP Address:port	Inside Global IP Address:port	Outside Global IP Address:port	Outside Global IP Address:port
TCP	10.1.1.2:1600	172.2.2.2:1399	2.2.2.2:25	2.2.2.2:25
TCP	10.1.1.1:1027	172.2.2.2:1280	1.1.1.1:25	1.1.1.1:25

图 6-12　动态 PAT

第 1 步：定义内网接口和外网接口。

```
Router(config-if)#ip nat inside
Router(config-if)#ip nat outside
```

第 2 步：定义内部本地地址范围。

```
Router(config)#access-list 10 permit 10.1.1.0 0.0.0.255
```

第 3 步：定义内部全局地址池。

```
Router(config)#ip nat pool abc 172.2.2.2 172.2.2.2 netmask 255.255.255.0
```

第 4 步：建立映射关系。

```
Router(config)#ip nat inside source list 10 pool abc overload
```

注意：PAT 在第四步建立映射关系时必须使用 overload 关键字，否则路由器将执行动态 NAT 转换。

（4）验证和诊断 NAT

显示翻译统计：

```
show ip nat statistics
```

显示活动翻译：

```
show ip nat translations
```

从 NAT 转换表中清除所有动态地址转换项：

```
clear ip nat translation *
```

6．PPP 协议

1）PPP 协议概述

PPP 协议是提供在点到点链路上承载网络层数据包的一种链路层协议。PPP 定义了一整套的协议包括链路控制协议（LCP）、网络层控制协议（NCP）和验证协议（PAP 和 CHAP）。PPP 由于能够提供用户验证、易于扩充和支持同异步而获得较广泛的应用。PPP 协议位于 OSI 七层模型的数据链路层，PPP 协议按照功能划分为两个子层：LCP、NCP。LCP 主要负责链路的协商、建立、回拨、认证、数据的压缩、多链路捆绑等功能。NCP 主要负责和上层的协议进行协商，为网络层协议提供服务。

PPP 的认证功能是指在建立 PPP 链路的过程中进行密码的验证，验证通过建立连接，验证不通过拆除链路。

PPP 协议支持两种认证方式 PAP 和 CHAP。PAP（Password Authentication Protocol，密码验证协议）是指验证双方通过两次握手完成验证过程，它是一种用于对试图登录到点对点协议服务器上的用户进行身份验证的方法。由被验证方主动发出验证请求，包含了验证的用户名和密码。由验证方验证后做出回复，通过验证或验证失败。在验证过程中用户名和密码以明文的方式在链路上传输。

2）PPP 协议的验证方式

PPP 支持两种验证方式：PAP 和 CHAP

（1）PAP 为两次握手验证，如图 6-13 所示，口令为明文。PAP 验证过程如下：

- 被验证方发送用户名和口令到验证方；
- 验证方根据用户配置查看是否有此用户以及口令是否正确，然后返回不同的响应。

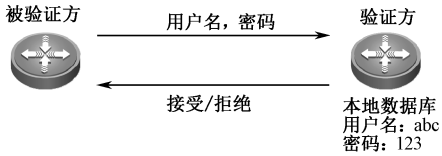


图 6-13　PAP 验证两次握手

（2）CHAP 为三次握手验证，如图 6-14 所示口令为密文（密钥）。CHAP 验证过程如下。

- 验证方向被验证方发送一些随机产生的报文；
- 被验证方用自己的口令字和 MD5 算法对该随机报文进行加密，将生成的密文发回验证方；
- 验证方用自己保存的被验证方口令字和 MD5 算法对原随机报文加密，比较二者的密文，根据比较结果返回不同的响应。

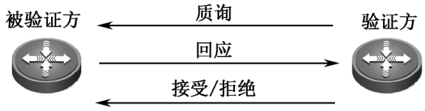


图 6-14　CHAP 三次握手

3）配置 PPP 协议

（1）配置 PPP PAP（见图 6-15）

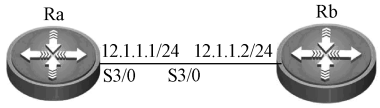


图 6-15　PAP 验证

```
Red-Giant(config)#hostname Ra
Ra(config)# interface serial 3/0
Ra(config-if)#ip address 12.1.1.1 255.255.255.0
```

```
Ra(config-if)#no shutdown
Red-Giant(config)#hostname Rb
Rb(config)# interface serial 1/2
Rb(config-if)#ip address 1.1.1.2 255.255.255.0
Rb(config-if)#clock rate 64000
Rb(config-if)#no shutdown
```

验证测试：（以 Ra 为例）

```
Ra#show interface serial 3/0
rial 3/0 is UP  , line protocol is UP
Hardware is PQ2 SCC HDLC CONTROLLER serial
Interface address is: 1.1.1.1/24
MTU 1500 bytes, BW 2000 Kbit
Encapsulation protocol is HDLC, loopback not set
Keepalive interval is 10 sec , set
Carrier delay is 2 sec
RXload is 1 ,Txload is 1
Queueing strategy: WFQ
5 minutes input rate 11 bits/sec, 0 packets/sec
5 minutes output rate 11 bits/sec, 0 packets/sec
33 packets input, 726 bytes, 0 no buffer
Received 33 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
32 packets output, 704 bytes, 0 underruns
0 output errors, 0 collisions, 6 interface resets
3 carrier transitions
V.35 DTE cable
DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

4）配置 PPP PAP 认证

被验证方的配置：

```
Ra(config)# interface serial 1/2
Ra(config-if)# encapsulation ppp     // 接口下封装 PPP 协议
Ra(config-if)#ppp pap sent-username Ra password 0 star
// PAP 认证的用户名、密码，该用户名和密码是从 Ra 上发送给 Rb 的用户名和密码
```

验证方的配置：

```
Rb(config)#username Ra password 0 cisco
//验证方配置被验证方用户名、密码，该用户名和密码一定要和从 Rb 上发送过来的用户名和密码相同
Rb(config-if)# encapsulation ppp
Rb(config-if)#ppp authentication pap  // PPP 启用 PAP 认证方式
```

验证测试：

```
Ra#debug ppp authentication        // 观察 PAP 验证过程
%LINK CHANGED: Interface serial 3/0, changed state to down
%LINE PROTOCOL CHANGE: Interface serial 3/0, changed state to DOWN
PPP: ppp_clear_author(), protocol %LINK CHANGED: Interface serial 3/0, changed
state to up
PPP: serial 3/0 PAP ACK received
PPP: serial 3/0 Passed PAP authentication with remote
PPP: serial 3/0 lcp authentication OK!
PPP: ppp_clear_author(), protocol = TYPE_IPCP
= TYPE_LCP
%LINE PROTOCOL CHANGE: Interface serial 3/0, changed state to UP
```

注意事项

1．在 DCE 端要配置时钟；

2．在接口下封装 PPP；

3．“debug ppp authentication”，在路由器物理层 up，链路尚未建立的情况下打开才有信息输出，本实验的实质是链路层协商建立的安全性，该信息出现在链路协商的过程中。

参考配置

```
Ra#show running-config              //路由器 Ra 配置
Building configuration...
Current configuration : 483 bytes
!
version 8.32(building 53)
hostname Ra
!
interface serial 3/0
encapsulation PPP
ppp pap sent-username Ra password 0 cisco
ip address 1.1.1.1 255.255.255.0
!
interface serial 1/3
clock rate 64000
!
interface FastEthernet 1/0
duplex auto
speed auto
!
interface FastEthernet 1/1
duplex auto
speed auto
!
interface Null 0
```

```
!
line con 0
line aux 0
line vty 0 4
login
!
end
Rb#show running-config            //路由器 Rb 配置
Building configuration...
Current configuration : 469 bytes
!
version 8.32(building 53)
hostname Rb
!
username Ra password 0 cisco
!
interface serial 3/0
encapsulation PPP
ppp authentication pap
ip address 1.1.1.2 255.255.255.0
clock rate 64000
!
interface serial 1/3
!
interface FastEthernet 1/0
duplex auto
speed auto
!
interface FastEthernet 1/1
duplex auto
speed auto
!
interface Null 0
!
line con 0
line aux 0
line vty 0 4
login
!
end
```

1．配置 CHAP 验证（见图 6-16）。

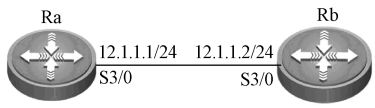


图 6-16　CHAP 验证

```
Red-Giant(config)#hostname Ra
Ra(config)# interface serial 3/0
Ra(config-if)#ip address 12.1.1.1 255.255.255.0
Ra(config-if)#no shutdown
Red-Giant(config)#hostname Rb
Rb(config)# interface serial 3/0
Rb(config-if)#ip address 12.1.1.2 255.255.255.0
Rb(config-if)#clock rate 64000
Rb(config-if)#no shutdown
验证测试：(以 Ra 为例)
Ra#show interface serial 3/0
serial 3/0 is UP  , line protocol is UP
Hardware is PQ2 SCC HDLC CONTROLLER serial
Interface address is: 12.1.1.1/24
  MTU 1500 bytes, BW 2000 Kbit
  Encapsulation protocol is HDLC, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  RXload is 1 ,Txload is 1
 Queueing strategy: WFQ
 5 minutes input rate 11 bits/sec, 0 packets/sec
 5 minutes output rate 11 bits/sec, 0 packets/sec
 33 packets input, 726 bytes, 0 no buffer
 Received 33 broadcasts, 0 runts, 0 giants
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
 32 packets output, 704 bytes, 0 underruns
 0 output errors, 0 collisions, 6 interface resets
 3 carrier transitions
 V35 DTE cable
 DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

2．配置 PPP CHAP 认证。

```
Ra(config)#username Rb password 0 cisco
Ra(config)#interface serial 3/0
Ra(config-if)#encapsulation ppp
Ra(config-if)#ppp authentication chap          // PPP 启用 CHAP 方式验证
Ra(config-if)#ppp chap hostname Ra
//配置 chap 验证的用户名，必须和另一路由上配置的 username 相同
Ra(config-if)#ppp chap password 0 cisco
//  0 表示加密等级，有 0 和 7 级，其中 0 表示没有加密，7 表示加密。
//输入验证口令，必须和对方 username 的口令一样
Rb(config)#interface serial 3/0
Rb(config-if)# encapsulation ppp
Ra(config-if)#ppp authentication chap
Ra(config-if)#ppp chap hostname Rb
Ra(config-if)#ppp chap password 0 cisco
```

验证测试：

```
Ra#debug ppp authentication              // 观察 CHAP 验证过程
%LINK CHANGED: Interface serial 3/0, changed state to down
%LINE PROTOCOL CHANGE: Interface serial 3/0, changed state to DOWN
PPP: ppp_clear_author(), protocol = TYPE_LCP
%LINK CHANGED: Interface serial 3/0, changed state to up
PPP: serial 3/0 Send CHAP challenge id=29 to remote host
PPP: serial 3/0 authentication event enqueue ,message type = [RECV_CHAP_RESPONSE]
PPP: dispose authentication message [RECV_CHAP_RESPONSE]
PPP: serial 3/0 CHAP response id=29 ,received from Rb
PPP: serial 3/0 Send CHAP success id=29 to remote
PPP: serial 3/0 remote router passed CHAP authentication.
PPP: serial 3/0 lcp authentication OK!
PPP: ppp_clear_author(), protocol = TYPE_IPCP
%LINE PROTOCOL CHANGE: Interface serial 3/0, changed state to UP
```

注意事项

1．在 DCE 端要配置时钟；

2．Ra(config)#username Rb password 0 cisco !username 后面的参数是对方的主机名；

3．Rb(config)#username Ra password 0 cisco !username 后面的参数是对方的主机名；

4．在接口下封装 PPP；

5．“debug ppp authentication”，在路由器物理层 up，链路尚未建立的情况下打开才有信息输出，本实验的实质是链路层协商建立的安全性，该信息出现在链路协商的过程中。

参考配置

```
Ra#show running-config                  //路由器 Ra 配置
Building configuration...
Current configuration : 489 bytes
!
version 8.32(building 53)
hostname Ra
!
username Rb password 0 cisco
!
interface serial 3/0
encapsulation PPP
ppp authentication chap
ip address 12.1.1.1 255.255.255.0
clock rate 64000
!
interface serial 4/0
clock rate 64000
!
interface FastEthernet 0/0
```

```
duplex auto
speed auto
!
interface FastEthernet 0/1
duplex auto
speed auto
!
interface Null 0
!
line con 0
line aux 0
line vty 0 4
login
!
end
Rb#show running-config                    // 路由器 Rb 配置
Building configuration...
Current configuration : 444 bytes
!
version 8.32(building 53)
hostname Rb
!
username Ra password 0 cisco
!
interface serial 3/0
encapsulation PPP
ip address 1.1.1.2 255.255.255.0
!
interface serial 4/0
clock rate 64000
!
interface FastEthernet 0/0
duplex auto
speed auto
!
interface FastEthernet 0/1
duplex auto
speed auto
!
interface Null 0
!
line con 0
line aux 0
line vty 0 4
login
!
```

（3）验证和诊断 PPP。

检查二层的封装，同时也可以显示 LCP 和 NCP 两者的状态。

```
Router#show interface serial
```

观察 PPP 通讯信程中的报文信息

```
Router#debug ppp packets
```

查看在 PPP 通信过程中的授权调试信息

```
Router#degub ppp authentication
```

项目实施

任务一　实现集团公司内部网络互通

任务描述

你是网络管理员，广州分公司业务的迅速发展，人员增加到 50 多人，原来的 sohu 路由器不能满足上网需求和与总公司网络互连的要求，现在已将 ADSL 接入改造为光纤接入。请你配置该网络实现广州分公司连接因特网。

网络拓扑

广州分公司网络拓扑如图 6-17 所示。

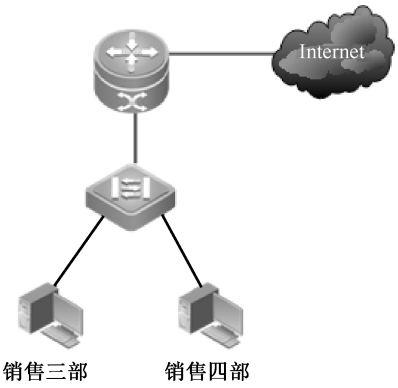


图 6-17　广州分公司拓扑图

任务目标

通过配置 NAT 协议，实现广州分公司连通 Internet。

设备清单

二层交换机 1 台、路由器 1 台。

【工作过程】:

步骤一：按照网络拓扑结构图，正确连接网络设备。

步骤二：IP 地址规划表

设　备	VLAN	IP	接口/说明
销售三部电脑	Vlan80	10.0.8.0/24	Fa0/1-10
销售四部电脑	Vlan90	10.0.9.0/24	Fa0/11-20
路由器	F0/0.1	10.0.8.254/24	子接口
	F0/0.2	10.0.9.254/24	子接口
	F0/1	100.1.2.2/30	外网接口

步骤三：配置交换机

```
Switch>enable
Switch#config t
Switch(config)#vlan 80
Switch(config-vlan)#exit
Switch(config)#int range fa0/1-10
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 80
Switch(config-if-range)#exit
Switch(config)#vlan 90
Switch(config-vlan)#exit
Switch(config)#int range fa0/11-20
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 90
Switch(config-if-range)#exit
Switch(config)#
Switch(config)#interface fa0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan all
Switch(config-if)#exit
Switch(config)#exit
Switch#write
```

步骤四：配置路由器子接口

```
Router>enable
Router#config ter  //进入全局配置模式
Router(config)#interface fa0/0.1   //进入子接口 fa0/0.1
Router(config-subif)#encapsulation dot1q 80  //封装 802.1Q，指定 Fa0/0.1 属于 VLAN 80
Router(config-subif)#ip address 10.0.8.254  255.255.255.0  //设置子接口的 IP 地址
Router(config-subif)#no shutdown  //激活端口
Router(config-subif)#exit
Router(config)#interface fa0/0.2
Router(config-subif)#encapsulation dot1q 90  //封装 802.1Q，指定 Fa0/0.2 属于 VLAN 90
Router(config-subif)#ip address 10.0.9.254 255.255.255.0 //设置子接口 IP 地址
Router(config-subif)#no shutdown
Router(config-subif)#exit
Router(config)#int fa0/1
Router(config-if)#ip address 100.1.2.2 255.255.255.252
```

```
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface fa0/0
Router(config-if)#no shutdown    //激活端口
Router(config)#interface fa0/0
```

步骤五：配置 NAT

```
Router(config)#access-list 1 permit 10.0.8.0 0.0.0.255
Router(config)#access-list 1 permit 10.0.9.0 0.0.0.255
Router(config)#ip nat inside source list 1 interface fa0/1 overload
Router(config)#int fa0/1
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#int fa0/0.1
Router(config-subif)#ip nat inside
Router(config-subif)#exit
Router(config)#int fa0/0.2
Router(config-subif)#ip nat inside
Router(config-subif)#exit
Router(config)#ip route 0.0.0.0 0.0.0.0 100.1.2.1 //配置默认路由
Router(config)#exit
Router#wr
Building configuration...
[OK]
```

项目测试

第一步：在销售三部的 PC 上利用 Ping 命令，测试到 ISP 商的网关，如图 6-18 所示。

```
PC>ping 100.1.2.1

Pinging 100.1.2.1 with 32 bytes of data:

Reply from 100.1.2.1: bytes=32 time=94ms TTL=127
Reply from 100.1.2.1: bytes=32 time=94ms TTL=127
Reply from 100.1.2.1: bytes=32 time=78ms TTL=127
Reply from 100.1.2.1: bytes=32 time=94ms TTL=127

Ping statistics for 100.1.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 78ms, Maximum = 94ms, Average = 90ms
```

图 6-18　测试到 ISP 商网关的连通性

任务二　实现集团公司与分公司互联

任务描述

你是网络管理员，现集团公司向 ISP 商租用了专线，将总公司与分公司之间的网络进行了连通。现需要在总公司与公司的路由器上配置动态路由协议，实现三地网络的通信。为了防止非法路由器接入到公司的网络，所以需要在三地的路由器间配置 PPP 认证，以提高网络的安全性。

北京总公司通过增加一台路由器与分公司之间进行互连。广州分公司和上海分公司已有路由器，只需将专线接入路由器即可与总公司连通。该方案的网络拓扑如图 6-4 所示。

其网络拓扑结构如图 6-19 所示。

网络拓扑

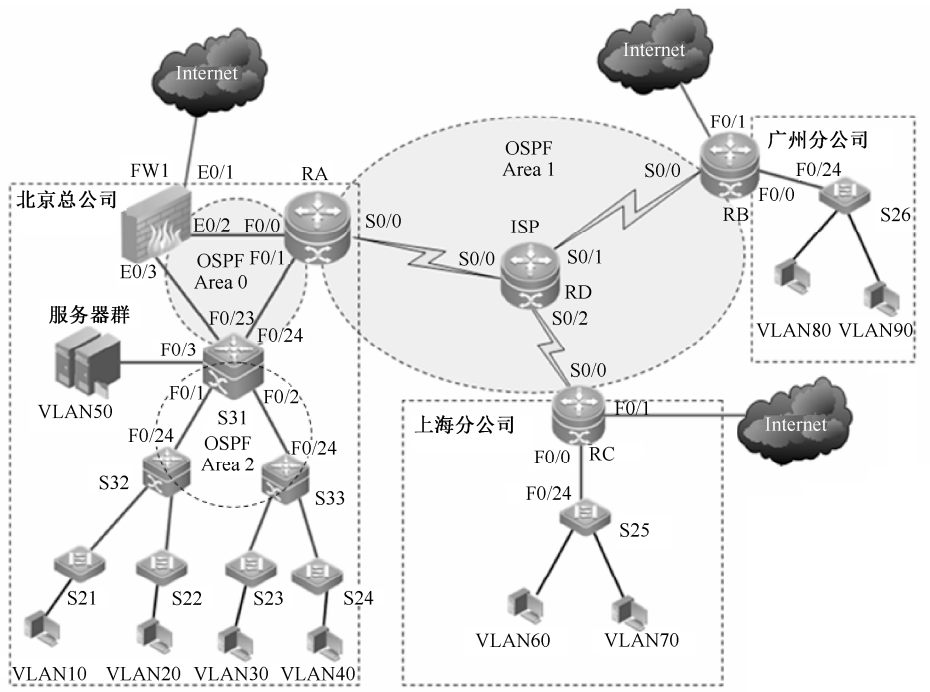


图 6-19 实现集团公司网络连接拓扑结构图

任务目标

1．在路由器上配置 OSPF 动态路由协议，实现三地网络互通

2．在路由器上配置 PPP 的 CHAP 认证，保证网络安全，用户名和密码如下表所示。

设　备	用　户　名	密　码
RA	RA	xrjt
RB	RB	xrjt
RC	RC	xrjt
RD	RD	xrjt

设备清单

三层交换机 3 台、路由器 3 台、防火墙 1 台、二层交换机 6 台、线缆 N 条。

【工作过程】:

步骤一：按照网络拓扑结构图，正确连接网络设备。

步骤二：IP 地址规划表

设　备	接　口	IP	说　明
S31	F0/23	10.0.12.2/24	
	F0/24	10.0.13.2/24	
	F0/3	10.0.5.254/24	
	F0/1	10.0.10.1/24	
	F0/2	10.0.11.2/24	
S32	F0/24	10.0.10.2/24	
	VLAN10	10.0.1.254/24	
	VLAN20	10.0.2.254/24	
S33	F0/24	10.0.11.2/24	
	VLAN30	10.0.3.254/24	
	VLAN40	10.0.4.254/24	
FW1	E0/3	10.0.12.1/24	
	E0/2	10.0.14.1/24	
	E0/1	200.1.2.2/28	
RA	F0/0	10.0.14.2/24	
	F0/1	10.0.13.1/24	
	S0/0	10.0.15.2/24	DTE
RB	S0/0	10.0.17.2/30	DTE
	F0/0.1	10.0.8.254/24	子接口
	F0/0.2	10.0.9.254/24	子接口
	F0/1	100.1.2.2/30	外网接口
RC	S0/0	10.0.16.2/30	DTE
	F0/0.1	10.0.6.254/24	子接口
	F0/0.2	10.0.7.254/24	子接口
	F0/1	222.1.2.2/30	外网接口
RD	S0/0	10.0.15.1/24	DCE
	S0/1	10.0.17.1/24	DCE
	S0/2	10.0.16.1/24	DCE

步骤三：配置接入层交换机

```
s21(config)#vlan 10
s21(config-vlan)#exit
s21(config)#int range fa0/1-23
s21(config-if-range)#switchport mode access
s21(config-if-range)#switchport access vlan 10
```

```
s21(config-if-range)#exit
s21(config)#int fa0/24
s21(config-if)#switchport mode trunk
s21(config-if)#switchport trunk allowed vlan all
s21(config-if)#exit
s21(config-if)#end
s21#write
```

其它接入层交换机 S22、S23、S24、S25、S26 的配置同上。

步骤四：配置汇聚层交换机 S32

（1）配置 Trunk

```
S32(config)#int range fa0/1-2
S32(config-if-range)#switchport mode trunk
S32(config-if-range)#switchport trunk allowed vlan all
S32(config-if-range)#exit
```

（2）配置接口 IP 地址

```
S32(config)#int fa0/24
S32(config-if)#no switchport
S32(config-if)#ip address 10.0.10.2 255.255.255.0
S32(config-if)#no shutdown
S32(config-if)#vlan 10
S32(config-vlan)#exit
S32(config)#int vlan 10
S32(config-if)#ip address 10.0.1.254 255.255.255.0
S32(config-if)#exit
S32(config-if)#vlan 20
S32(config-vlan)#exit
S32(config)#int vlan 20
S32(config-if)#ip address 10.0.2.254 255.255.255.0
S32(config-if)#exit
```

（3）配置路由协议

```
S32(config)#router ospf 1   //开启 OSPF 动态路由协议，进程号为 1
S32(config-router)#network 10.0.1.0 0.0.0.255 area 2  //宣告网段
S32(config-router)#network 10.0.2.0 0.0.0.255 area 2
S32(config-router)#network 10.0.10.0 0.0.0.255 area 2
S32(config-router)#exit
S32(config)#ip route 0.0.0.0 0.0.0.0 10.0.10.1 //配置默认路由
S32(config)#end
S32#write
```

汇聚层交换机 S33 的配置同 S32，配置时注意 IP 地址的改变。

步骤五：配置核心层交换机 S31

（1）配置接口 IP 地址

```
S31(config)#int fa0/1
```

```
S31(config-if)#no switchport
S31(config-if)#ip address 10.0.10.1 255.255.255.0
S31(config-if)#no shutdown
S31(config)#int fa0/2
S31(config-if)#no switchport
S31(config-if)#ip address 10.0.11.1 255.255.255.0
S31(config-if)#no shutdown
S31(config-if)#int fa0/3
S31(config-if)#no switchport
S31(config-if)#ip address 10.0.5.254 255.255.255.0
S31(config-if)#no shutdown
S31(config-if)#int fa0/23
S31(config-if)#no switchport
S31(config-if)#ip address 10.0.12.2 255.255.255.0
S31(config-if)#no shutdown
S31(config-if)#int fa0/24
S31(config-if)#no switchport
S31(config-if)#ip address 10.0.13.2 255.255.255.0
S31(config-if)#no shutdown
```

（2）配置路由协议

```
S31(config)#router ospf 1
S31(config-router)#network 10.0.12.0 0.0.0.255 area 0
S31(config-router)#network 10.0.13.0 0.0.0.255 area 0
S31(config-router)#network 10.0.5.0 0.0.0.255 area 0
S31(config-router)#network 10.0.10.0 0.0.0.255 area 2
S31(config-router)#network 10.0.11.0 0.0.0.255 area 2
S31(config-router)#exit
S31(config)#ip route 0.0.0.0 0.0.0.0 10.0.12.1
S31(config)#end
S31#write
```

步骤六：配置防火墙 FW1

锐捷 RG-WALL 系列防火墙，运行 OSPF 协议需要在命令行模式下配置，具体如下：

（1）配置接口 IP 地址

```
RG-WALL#config t
RG-WALL(config)# int ge1
RG-WALL(config-ge1)#ip address 200.1.2.2/28
RG-WALL(config-ge1)#no shutdown
RG-WALL(config-ge1)#exit
RG-WALL(config)# int ge2
RG-WALL(config-ge2)#ip address 10.0.14.1/24
RG-WALL(config-ge2)#no shutdown
RG-WALL(config-ge2)#exit
RG-WALL(config)# int ge3
RG-WALL(config-ge3)#ip address 10.0.12.1/24
```

```
RG-WALL(config-ge3)#no shutdown
RG-WALL(config-ge3)#exit
```

（2）配置 OSPF 动态路由协议

```
RG-WALL(config)# router ospf
RG-WALL(router-ospf)# network 10.0.12.0/24
RG-WALL(router-ospf)# network 10.0.12.0/24 area 0
RG-WALL(router-ospf)# network 10.0.14.0/24 area 0
RG-WALL(router-ospf)# exit
RG-WALL# write memory
```

步骤六：配置路由器 RA

（1）配置接口 IP 地址

```
RA(config)#int fa0/0
RA(config-if)#ip address 10.0.14.2 255.255.255.0
RA(config-if)#no shut
RA(config-if)#int fa0/1
RA(config-if)#ip address 10.0.13.1 255.255.255.0
RA(config-if)#no shut
RA(config-if)#int s0/0
RA(config-if)#ip address 10.0.15.2 255.255.255.0
RA(config-if)#no shutdown
```

（2）配置 OSPF 动态路由协议

```
RA(config-if)#router ospf 1
RA(config-router)#network 10.0.13.0 255.255.255.0 area 0
RA(config-router)#network 10.0.14.0 255.255.255.0 area 0
RA(config-router)#network 10.0.15.0 255.255.255.0 area 1
RA(config-router)#exit
```

（3）配置 PPP 的 CHAP 认证

```
RA(config)#username RD password 0 xrjt     //配置用户名和密码
RA(config)#interface serial 0/0
RA(config-if)#encapsulation ppp       //封装 PPP 协议
RA(config-if)#ppp authentication chap         // PPP 启用 CHAP 方式验证
RA(config-if)#ppp chap hostname RA
RA(config-if)#end
RA#write
```

步骤七：配置路由器 RD

（1）配置接口 IP 地址

```
RD(config)#int s0/0
RD(config-if)#ip address 10.0.15.1 255.255.255.0
RD(config-if)#clock rate 64000
RD(config-if)#no shutdown
RD(config-if)#int s0/1
```

```
RD(config-if)#ip address 10.0.17.1 255.255.255.0
RD(config-if)#clock rate 64000
RD(config-if)#no shutdown
RD(config-if)#int s0/2
RD(config-if)#ip address 10.0.16.1 255.255.255.0
RD(config-if)#clock rate 64000
RD(config-if)#no shutdown
RD(config-if)#exit
```

（2）配置 OSPF 动态路由协议

```
RD(config)#router ospf 1
RD(config-router)#network 10.0.15.0 0.0.0.255 area 1
RD(config-router)#network 10.0.16.0 0.0.0.255 area 1
RD(config-router)#network 10.0.17.0 0.0.0.255 area 1
RD(config-router)#exit
```

（3）配置 PPP 的 CHAP 认证

```
RD(config)#username RA password 0 xrjt
RD(config)#username RB password 0 xrjt
RD(config)#username RC password 0 xrjt
RD(config)#interface serial 0/0
RD(config-if)#encapsulation ppp
RD(config-if)#ppp authentication chap
RD(config-if)#ppp chap hostname RD  （注意：在 cisco 设备中无此命令）
RD(config)#interface serial 0/1
RD(config-if)#encapsulation ppp
RD(config-if)#ppp authentication chap
RD(config-if)#ppp chap hostname RD
RD(config)#interface serial 0/2
RD(config-if)#encapsulation ppp
RD(config-if)#ppp authentication chap
RD(config-if)#ppp chap hostname RD
RD(config-if)#end
RD#write
```

步骤八：配置路由器 RB

广州分公司的网络中内网通信部份配置请参照任务一。

（1）配置 S0/0 接口 IP 地址

```
RB(config)#int s0/0
RB(config-if)#ip address 10.0.17.2 255.255.255.0
RB(config-if)#no shutdown
```

（2）配置 OSPF 动态路由协议

```
RB(config-if)#router ospf 1
RB(config-router)#network 10.0.17.0 0.0.0.255 area 1
RB(config-router)#network 10.0.8.0 0.0.0.255 area 1
```

```
RB(config-router)#network 10.0.9.0 0.0.0.255 area 1
RB(config-router)#exit
```

（3）配置 PPP 的 CHAP 认证

```
RB(config)#username RD password 0 xrjt
RB(config)#int s0/0
RB(config-if)#encapsulation ppp
RB(config-if)#ppp authentication chap
RB(config-if)#ppp chap hostname RB  （注意：在 cisco 设备中无此命令）
RB(config-if)#exit
RB(config-if)#end
RB#write
```

步骤九：配置路由器 RC

上海分公司的网络中内网通信部份配置请参照任务一。

（1）配置 S0/0 接口 IP 地址

```
RC(config)#int s0/0
RC(config-if)#ip address 10.0.16.2 255.255.255.0
RC(config-if)#no shutdown
```

（2）配置 OSPF 动态路由协议

```
RC(config-if)#router ospf 1
RC(config-router)#network 10.0.16.0 0.0.0.255 area 1
RC(config-router)#network 10.0.6.0 0.0.0.255 area 1
RC(config-router)#network 10.0.7.0 0.0.0.255 area 1
RC(config-router)#exit
```

（3）配置 PPP 的 CHAP 认证

```
RC(config)#username RD password 0 xrjt
RC(config)#int s0/0
RC(config-if)#encapsulation ppp
RC(config-if)#ppp authentication chap
RC(config-if)#ppp chap hostname RC  （注意：在 cisco 设备中无此命令）
RC(config-if)#exit
RC(config-if)#end
RC#write
```

注意：如要实现北京总公司的电脑连接互联网还需要做防火墙的 NAT 配置，防火墙的 NAT 配置将在项目七中阐述。

【项目测试】：

1．在总公司核心路由器上通过 show ip route 命令可以查看到所有网段的路由信息。

```
S31#sho ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGPD - EIGRP,
EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

```
    N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2   E1 - OSPF external
type 1, E2 - OSPF external type 2, E - EGP  i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS
level-2, ia - IS-IS inter area
     * - candidate default, U - per-user static route, o - ODR P - periodic downloaded
static route
        10.0.0.0/24 is subnetted, 17 subnets
    O      10.0.1.0 [110/2] via 10.0.10.2, 01:44:23, FastEthernet0/1
    O      10.0.2.0 [110/2] via 10.0.10.2, 01:44:23, FastEthernet0/1
    O      10.0.3.0 [110/2] via 10.0.11.2, 01:44:23, FastEthernet0/2
    O      10.0.4.0 [110/2] via 10.0.11.2, 01:44:23, FastEthernet0/2
    C      10.0.5.0 is directly connected, FastEthernet0/3
    O IA   10.0.6.0 [110/130] via 10.0.13.1, 00:03:35, FastEthernet0/24
    O IA   10.0.7.0 [110/130] via 10.0.13.1, 00:03:35, FastEthernet0/24
    O IA   10.0.8.0 [110/130] via 10.0.13.1, 00:03:35, FastEthernet0/24
    O IA   10.0.9.0 [110/130] via 10.0.13.1, 00:03:35, FastEthernet0/24
    C      10.0.10.0 is directly connected, FastEthernet0/1
    C      10.0.11.0 is directly connected, FastEthernet0/2
    C      10.0.12.0 is directly connected, FastEthernet0/23
    C      10.0.13.0 is directly connected, FastEthernet0/24
    O      10.0.14.0 [110/2] via 10.0.12.1, 01:44:18, FastEthernet0/23
                     [110/2] via 10.0.13.1, 01:44:18, FastEthernet0/24
    O IA   10.0.15.0 [110/65] via 10.0.13.1, 01:18:26, FastEthernet0/24
    O IA  10.0.16.0 [110/129] via 10.0.13.1, 00:03:35, FastEthernet0/24
    O IA  10.0.17.0 [110/129] via 10.0.13.1, 00:03:35, FastEthernet0/24
    S*  0.0.0.0/0 [1/0] via 10.0.12.1
```

2．在总公司的任意 PC 上通过 tracert 命令，可以测试到广州分公司网络所经过的路径是 S32→S31→RA→RD→RA→PC

认证测试

一、选择题

1．下列不属于动态路由协议的是（　　）。

A．ICMP　　B．RIP　　C．OSPF　　D．IS-IS

2．RIP 协议是基于（　　）。

A．TCP　　B．UDP　　C．ICMP　　D．IP

3．RIP 协议可以到的目标网络的跳数（所经过路由器的个数）最多为（　　）。

A．14　　B．15　　C．16　　D．无限制

4．RIP 协议的路由项在（　　）时间内没有更新会变为不可达？

A．90s　　B．120s　　C．180s　　D．240s

5．关闭 RIP 路由汇总的命令是（　　）。

A．no auto-summary　　B．auto-summary

C．no shutdown　　D．no ip router

6．OSPF（开放式最短路径优先协议）采用（　　）算法计算最佳路由。

A．Spanning-Tree　B．Bellman-Ford　　C．Dijkstra　　D．Dynamic-Search

7．以下关于 OSPF 协议的描述中，最正确的是（　　）。

A．OSPF 协议根据链路状态法计算最佳路由

B．OSPF 协议是用于自治系统之间的外部网关协议

C．OSPF 协议不能根据网络通信情况动态地改变路由

D．OSPF 协议只能适用于小型网络

8．下列关于 PPP 协议的说法正确的是（　　）。

A．PPP 协议是一种 NCP 协议

B．PPP 协议与 HDLC 同属广域网协议

C．PPP 协议只能工作在同步串行链路上

D．PPP 协议是三层协议

9．以下封装协议使用 CHAP 或者 PAP 验证方式的是（　　）。

A．HDLC　　B．PPP　　C．SDLC　　D．SLIP

10．（　　）为两次握手协议，它通过在网络上以明文的方式传递用户名及口令来对用户进行验证。

A．PAP　　B．CHAP　　C．IPCP　　D．RADIUS

11．某公司需要将自己的 Web 服务器挂载到 Internet 上供他人访问，该选择哪一种类型的 NAT（　　）？

A．静态 NAT　　B．动态 NAT　　C．PAT　　D．不使用 NAT

12．下列关于 NAT 缺点描述中，正确的是（　　）。

A．NAT 增加了延时。

B．保护了内部网络结构。

C．通过内部地址私有化来节约合法的注册寻址方案

D．使得 NAT 设备维护一个地址转换表，把私有的 IP 地址映射到合法的 IP 地址上。

二、简答题

1．简述 RIPv1 和 RIPv2 的区别？

2．OSPF 比 RIP 有哪些优势？

3．简述 PAP 的验证过程。

4．简述 CHAP 的验证过程。

5．在 NAT 中有哪四种地址？

6．动态 NAT 和 PAT 的主要区别是什么？

项目七　工业园区网络配置与管理

项目背景

数码工业园区是花都市新建的经济开发区中的一个，专门用于科技数码高新企业作为研发和生产的基地，占地近千亩。最近准备建设园区网，其覆盖范围包括多栋高层写字楼以及园区办公楼等建筑，入驻企业规模大小不等，现有 2500 个左右的信息点。企业由于自建机房的成本太高，自己拥有服务器等的企业希望就近托管，以便维护，没有服务器的企业希望能就近租用到安全、可靠的服务器，园区内企业对数据链路的要求高，特别要求网络要具备链路冗余和负载均衡的功能，企业接入网络方便，能够有效隔离其他企业的影响；而且由于园区正在进一步扩大，园区内路由协议要动态适应网络结构的变化，以便在连接新建筑网络时，减少对原有用户的影响；数码工业园区的蔡主任，已成立了园区网络维护中心，由中心的李工程师带领中心技术人员来完成这个任务。

项目分析

分析如下：

（1）数据交换与通信。发布园区内的政策、制度、通知等各项信息，链接相关的平台，提供互联网接入功能。

（2）服务器托管与租赁。园区中心服务器机房的建设，可以给企业提供就近服务器托管和租赁业务，方便企业使用和维护。

（3）资源共享。园区采用主流技术建设，能够提供高速的数据传递，使得园区网内进行的资源共享（如上传和下载）变得更加方便和快捷。

（4）提高系统的可靠性。在一些用于计算机实时控制和高可靠性要求的场合，通过计算机网络技术实现备份技术可以提高系统的可靠性，可实现分布式网络处理和负载均衡。

项目方案

数码工业园区网络属于大型园区网，典型的园区网包括校园网、社区网、住宅小区网、工业园区网等，园区网由于信息点和网络设备都比较多，管理复杂，经过李工的团队商议，决定采用混合型网络拓扑结构，如图 7-1 所示；其他具体参数如下：

（1）通过系统的 IP 地址规则，使得园区网络的 IP 地址分配合理、有序，使用 NAT 功能，结合私有 IP 地址的使用减少 IP 地址的浪费。

（2）通过园区网内的二、三层交换机，实现内部新网络的路由和交换，通过对网络设备的体系化配置，使得网络设备运行更稳定、更安全、可扩展性强，保证整个园区网络的平稳运行，便于管理与维护。

（3）通过配置防火墙的相关配置实现连接因特网，将托管服务器放入 DMZ 区域，有效保证服务器的数据安全，并且配置安全策略、防攻击保护等措施实现整个网络的安全运行。

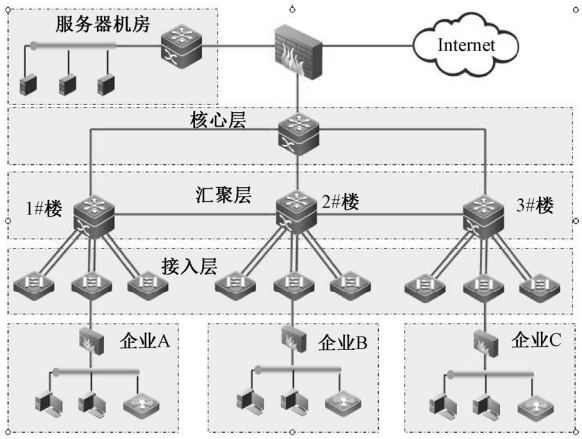


图 7-1　网络拓扑图

知识准备

1．硬件防火墙技术

1）什么是硬件防火墙？

把软件防火墙嵌入在硬件中，一般的软件安全厂商所提供的硬件防火墙便是在硬件服务器厂商定制硬件，然后再把 Linux 系统与自己的软件系统嵌入（Symantec 的 SGS 便是 DELL+Symantec 的软件防火墙）。这样做的好处是 Linux 相对 Windows 的 Server 相对安全。这样做的理由是由于 ISA 必须装在 Windows 操作系统下，微软的操作系统相对不安全，本身存在安全隐患的系统上部署安全策略相当于处在亚安全状态，是不可靠的。在兼容性方面也是硬件防火墙更胜一筹，其实软件防火墙与硬件防火墙的主要区别就在于硬件。硬件防火墙是保障内部网络安全的一道重要屏障。它的安全和稳定，直接关系到整个内部网络的安全。因此，日常例行的检查对于保证硬件防火墙的安全是非常重要的。系统中存在的很多隐患和故障在暴发前都会出现这样或那样的苗头，例行检查的任务就是要发现这些安全隐患，并尽可能将问题定位，方便问题的解决。

2）硬件防火墙的工作原理

（1）包过滤防火墙

包过滤防火墙一般在路由器上实现，用以过滤用户定义的内容，如 IP 地址。包过滤防火墙的工作原理是：系统在网络层检查数据包，与应用层无关。这样系统就具有很好的传输性能，可扩展能力强。但是，包过滤防火墙的安全性有一定的缺陷，因为系统对应用层信息无感知，也就是说，防火墙不理解通信的内容，所以可能被黑客所攻破，如图 7-2 所示。

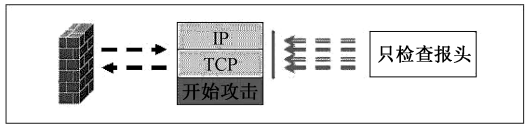


图 7-2　包过滤防火墙工作原理图

（2）应用网关防火墙

应用网关防火墙检查所有应用层的信息包，并将检查的内容信息放入决策过程，从而提高网络的安全性。然而，应用网关防火墙是通过打破客户机 / 服务器模式实现的。每个客户

机 / 服务器通信需要两个连接：一个是从客户端到防火墙，另一个是从防火墙到服务器。另外，每个代理需要一个不同的应用进程，或一个后台运行的服务程序，对每个新的应用必须添加针对此应用的服务程序，否则不能使用该服务。所以，应用网关防火墙具有可伸缩性差的缺点，如图 7-3 所示。

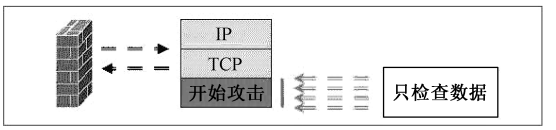


图 7-3　应用网关防火墙工作原理图

（3）状态检测防火墙

状态检测防火墙基本保持了简单包过滤防火墙的优点，性能比较好，同时对应用是透明的，在此基础上，对于安全性有了大幅提升。这种防火墙摒弃了简单包过滤防火墙仅仅考察进出网络的数据包，不关心数据包状态的缺点，在防火墙的核心部分建立状态连接表，维护了连接，将进出网络的数据当成一个个事件来处理。可以这样说，状态检测包过滤防火墙规范了网络层和传输层行为，而应用代理型防火墙则是规范了特定的应用协议上的行为，如图 7-4 所示。

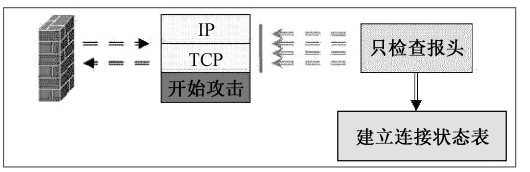


图 7-4　状态检测防火墙工作原理图

（4）复合型防火墙

复合型防火墙是指综合了状态检测与透明代理的新一代的防火墙，进一步基于 ASIC 架构，把防病毒、内容过滤整合到防火墙里，其中还包括 VPN、IDS 功能，多单元融为一体，是一种新突破。常规的防火墙并不能防止隐蔽在网络流量里的攻击，在网络界面对应用层扫描，把防病毒、内容过滤与防火墙结合起来，这体现了网络与信息安全的新思路。它在网络边界实施 OSI 第七层的内容扫描，实现了实时在网络边缘布署病毒防护、内容过滤等应用层服务措施，如图 7-5 所示。

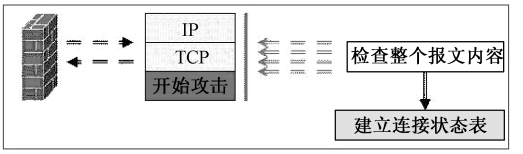


图 7-5　复合型防火墙工作原理图

2．硬件防火墙技术

1）下一代防火墙技术

现在的防火墙不同于传统防火墙，在网络安全的实际应用中，单一的安全防护技术并不足以构筑一个安全的网络安全体系，多种技术的综合应用才能够将安全风险控制在尽量小的范围内。

目前的硬件防火墙已经发展到下一代防火墙技术（NGFW），一个线速（Wire-speed）网

络安全处理平台，具有以下特性。

（1）标准的第一代防火墙能力：包过滤、网络地址转换（NAT）、状态性协议检测、VPN 等。

（2）集成的而非仅仅共处一个位置的网络入侵检测：支持面向安全漏洞的特征码和面向威胁的特征码。IPS 与防火墙的互动效果应当大于这两部分效果的总和。例如提供防火墙规则来阻止某个地址不断向 IPS 加载恶意传输流。这个例子说明，在 NGFW 中，应该由防火墙建立关联，而不是操作人员去跨控制台部署解决方案。集成具有高质量的 IPS 引擎和特征码，是 NGFW 的一个主要特征。

（3）应用意识和全栈可见性：识别应用和在应用层上执行独立于端口和协议，而不是根据纯端口、纯协议和纯服务的网络安全政策。例子包括允许使用 Skype，但关闭 Skype 中的文件共享或始终阻止 GoToMyPC。

（4）额外的防火墙智能：防火墙收集外来信息做出更好的阻止决定或建立优化的阻止规则库。例子包括利用目录集成将阻止行为与用户身份绑在一起，或建立地址的黑白名单。Gartner 认为，随着防火墙和 IPS 更新周期的自然到来，或者随着带宽需求的增加和成功的攻击，促使更新防火墙，大企业将用 NGFW 替换已有的防火墙。不断变化的威胁环境，以及不断变化的业务和 IT 流程将促使网络安全经理在他们的下一个防火墙/IPS 更新周期时寻找 NGFW。

2）防火墙的技术革新

应用识别是防火墙未来发展的重要技术方向，基于应用的攻击不断变化，也要求防御技术必须有所提升。对于这样的变化，传统防火墙只能望而兴叹。因为它在应用层无法起到良好的防御效果，而 IPS 仅关注应用层检测，防火墙功能较弱，这也是有些用户把 IPS 当做 IDS 使用的一个原因。UTM 则是一个集成的产品，能够很好地融合各种安全技术。下一代防火墙在性能、安全性、易用性、可管理性等方面有了质的飞跃，满足用户新的防御和管理需求。

相比传统防火墙和 UTM，下一代防火墙与它们的主要区别在于：

（1）传统防火墙局限于 IP 地址、接口层面的安全防护。从基于简单包过滤技术防火墙到基于状态检测技术的防火墙，重点的防护还仅仅是停留在 OSI 模型的四层以内；

（2）UTM 是在“瘦防火墙”基础上发展而来的，集防火墙、IPS、VPN 等安全功能于一体的集成安全网关，其不足之处在于处理机制烦琐，效率低下，内部安全模块间缺少智能关联；

（3）下一代防火墙除了具备传统防火墙功能外，更关注针对应用层面的安全防护。实时性、准确性、高效性也成为下一代防火墙的主要特点。它会根据深度包检测引擎的检测结果，自动识别到该流量在应用层执行的安全策略。流量控制需要更“精细化”的管理，不仅仅能够对异常攻击流量进行阻止或允许动作，更可用来进行基于应用层的 QoS 控制，控制粒度更为细致。例如，可允许用户使用 Netmeeting 会议，但禁止其白板功能等，检测顺序也更为高效。设备对数据流仅需进行一次检测，IPS、FW 模块并行进行识别判断。

3．下一代防火墙配置

下一代防火墙相比传统防火墙与 UTM 防火墙来说，功能更强大，配置选项更多，如图 7-6 所示，可配置的选项有网络管理、路由管理、资源管理、防火墙、VPN、入侵防御、病毒防护、应用控制、内容过滤、反垃圾邮件等功能。管理员应该根据企业网络的现状，做出合适

的相应配置。

1）用 Web 登录硬件防火墙

IP 地址通常会在防火墙的配置手册中有说明，比如锐捷 1600 系列的防火墙的管理 IP 地址是：192.168.1.200/24。允许对该接口进行 Ping，Https 操作；系统默认的管理员用户为 admin，密码为 firewall。用户可以使用这个管理员账号从任何地址登录设备，并且使用设备的所有功能。

打开 IE，在地址栏输入：https://192.168.1.200 如图 7-7 所示。

图 7-6　下一代防火墙配置

图 7-7　登录防火墙

2）设置接口的 IP 地址

在导航栏中单击“网络管理”→“接口”→“接口”，在右边的窗口中进行相应的设置，如图 7-8 所示。

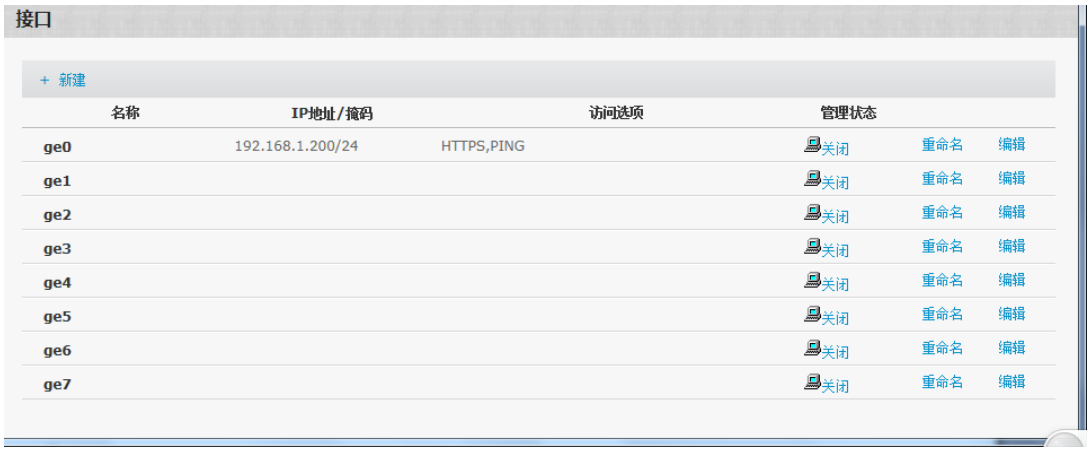


图 7-8　接口 IP 设置

3）设置安全域

在导航栏中单击“网络管理”→“接口”→“安全域”，在右边的窗口中单击“新建”按钮，如图 7-9 所示方式进行配置。

4）配置缺省网关和 DNS

在导航栏中单击“网络管理”→“基本配置”→“缺省网关”/“DNS”，在右边的窗口中，点击“新建”按钮，按如图 7-10 所示方式配置网关，按如图 7-11 所示方式配置 DNS 地址。

图 7-9　安全域设置

图 7-10　缺省网关设置

图 7-11　配置 DNS

5）NAT 的配置

NAT 分为源 NAT 和目的 NAT。

基于源地址的 NAT，可细分为动态 NAT、PAT 和静态 NAT。

动态 NAT 和 PAT 是一种单向的针对源地址的映射，主要用于内网访问外网，减少公有地址的数目，隐藏内部地址。动态 NAT 指动态地将源地址转换映射到一个相对较小的地址池中，对于同一个源 IP，不同的连接可能映射到地址池中不同的地址；PAT 是指将所有源地址都映射到同一个地址上，通过端口的映射实现不同连接的区分，实现公网地址的共享。

静态 NAT 是一种一对一的双向地址映射，主要用于内部服务器向外提供服务的情况。在这种情况下，内部服务器可以主动访问外部，外部也可以主动访问这台服务器，相当于在内、外网之间建立了一条双向通道。

基于目标地址的 NAT，我们称为目的 NAT，可分为目标地址映射、目标端口映射、服务器负载均衡等。基于目标地址的 NAT 也称为反向 NAT 或地址映射。目的 NAT 是一种单向的针对目标地址的映射，主要用于内部服务器向外部提供服务的情况，它与静态 NAT 的区别在于它是单向的。外部可以主动访问内部，内部却不可以主动访问外部。另外，可使用目的 NAT 实现负载均衡的功能，即可以将一个目标地址转换为多个内部服务器地址。也可以通过端口的映射将不同的端口映射到不同的机器上。另外，掌握 NAT 的基本原理之后，NAT 不仅仅可用于公有地址和私有地址之间的转换，还可用于公有地址与公有地址之间、私有地址与私有地址之间的转换。

例如：新建一个源地址转换的具体配置如下：

在导航栏中单击“网络管理”→“基本配置”→“NAT”，在右边的窗口中，单击“源地址转换”→“新建”，如图 7-12 和图 7-13 所示。

图 7-12　NAT 的配置

图 7-13　源 NAT 的配置

6）路由的配置

防火墙路由的配置有静态路由、动态路由和策略路由。

例如：配置一个出外的默认路由具体如下：

在导航栏中单击“路由管理”→“静态路由”→“静态路由”，在右边的窗口中，单击“新建”，如图 7-14 所示。

配置出外的默认路由通常还要配置“回指路由”，如果内网接口的 IP 是：192.168.255.2/30 的话，则配置如图 7-15 所示。

图 7-14　默认路由配置

图 7-15　回指路由配置

7）配置安全策略

通过配置安全策略，防火墙能够对经过设备的数据流进行有效的控制和管理。当防火墙收到数据报文时，把该报文的方向、源地址、目的地址、协议、端口等信息和用户配置的策略进行匹配，决定是否建立这条数据流，并且把这条流和匹配的策略关联起来，从而确定如何处理该流的后续报文，实现允许、丢弃、加密和解密、认证、排定优先次序、调度、过滤以及监控数据流，决定哪些用户和数据能进出，以及它们进出的时间和地点。

同时，在安全策略中还可以根据匹配结果，对符合规则的报文实行过滤动作（允许通过或丢弃），简单地实现包过滤功能。在没有配置任何安全策略的情况下，对于经过设备的所有数据包，其缺省策略为禁止。

安全策略按先配置先匹配的原则，只对通过设备的数据包进行处理，对于到设备本身的数据包和设备本身发出的数据包不进行限制。

例如：配置一条允许所有内网主机出外网的策略。

在导航栏中单击“防火墙”→“安全策略”→“安全策略”，在右边的窗口中，单击“新建”，如图 7-16 所示。

8）配置防攻击

在导航栏中单击“入侵防御”→“防攻击”→“配置”，在右边的窗口中，勾选相应选项，如图 7-17 所示。

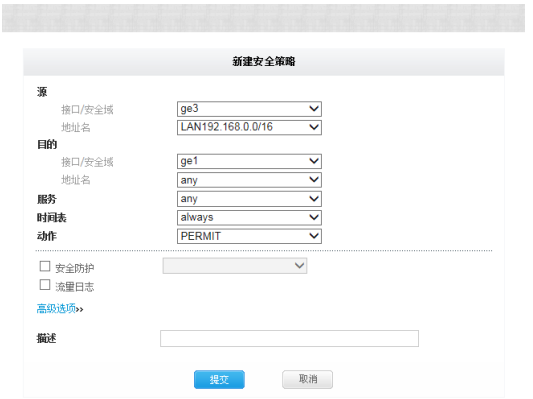


图 7-16 新建安全策略

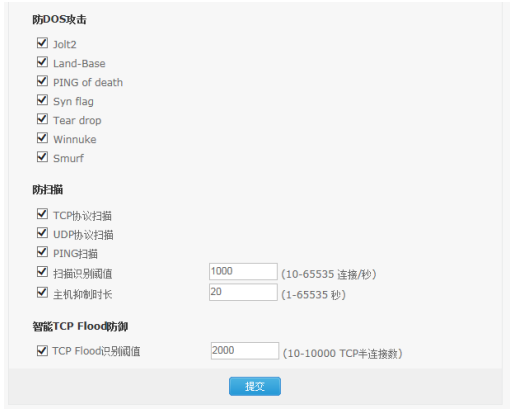


图 7-17 防攻击设置

9）设置内容过滤

在导航栏中单击“内容过滤”→“关键字过滤”，在右边的窗口中，输入相应文件，如“法轮功”，单击“新建”→“提交”，如图 7-18 所示。

图 7-18 过滤“法轮功”

10）根据企业网络要求，继续配置反垃圾邮件、VPN、反 P2P 设置等，最后单击“存盘”来保存配置，如图 7-19 所示。

图 7-19 单击“存盘”

项目实施

任务一 搭建数码工业园区网络

任务描述

数码工业园区是花都市新建的经济开发区中的一个，专门用于科技数码高新企业作为研发和生产的基地，占地近千亩，现有信息点近 2500 个，需要建设园区网。

网络拓扑

其网络拓扑如图 7-20 所示。

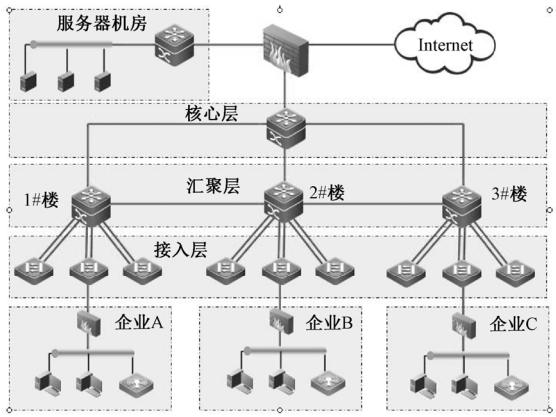


图 7-20　网络拓扑图

任务目标

要求合理规划 IP 地址，减少地址浪费；配置生成树和端口聚合，使网络具备链路冗余和负载均衡的功能；能够有效隔离其他企业的影响；使用动态路由协议适应网络结构的变化；并通过配置防火墙的相关配置实现安全连接 Internet。

设备清单

下一代防火墙 1 台、三层交换机 4 台、二层交换机 N 台、双绞线 N 条、计算机共 N 台。

工作过程

步骤一：地址规划及网络连通配置。

1）网络整体 IP 规划方案如图 7-21 所示。

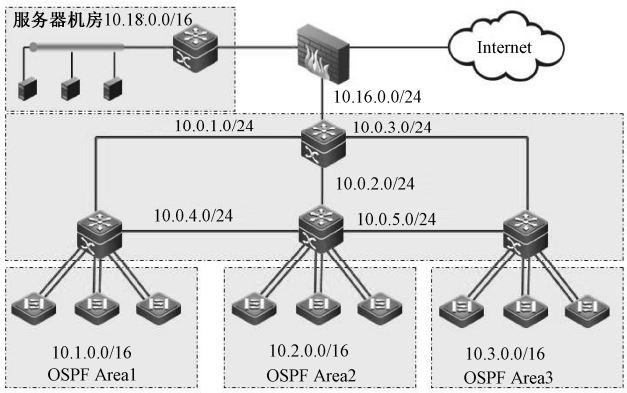


图 7-21　IP 地址规划表

2）网络设备名称及编号规则。

（1）修改核心层交换机设备名称为：SW-HX（其中 HX 表示为核心）如图 7-22 所示。

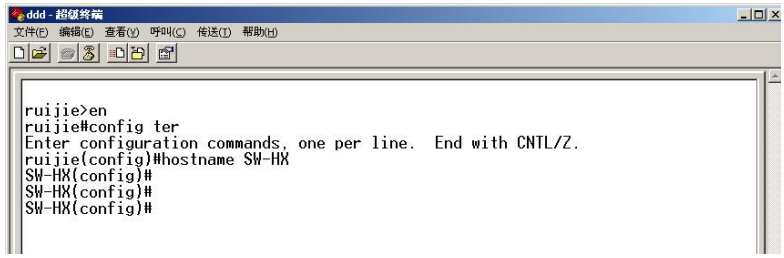
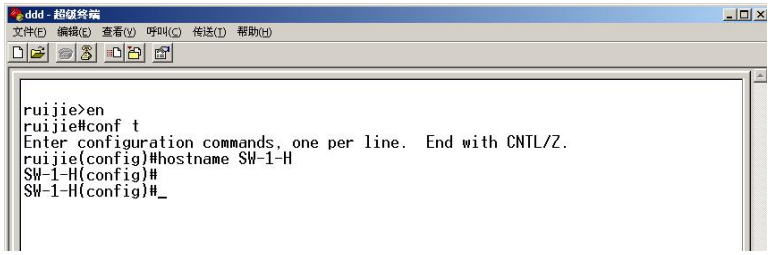


图 7-22 修改核心交换机名称

（2）汇聚层交换机依次为：SW-1-H 、SW-2-H 、SW-3-H（其中 1、2、3 表示建筑物的编号，H 表示汇聚），如图 7-23 所示。



7-23 修改汇聚层交换机地址

（3）接入层交换机依次为：SW-1-1、SW-1-2、SW-1-3…（其中 1、2、3 表示建筑物的编号，最后的数字表示该建筑物接入层交换机的编号），如图 7-24 所示。

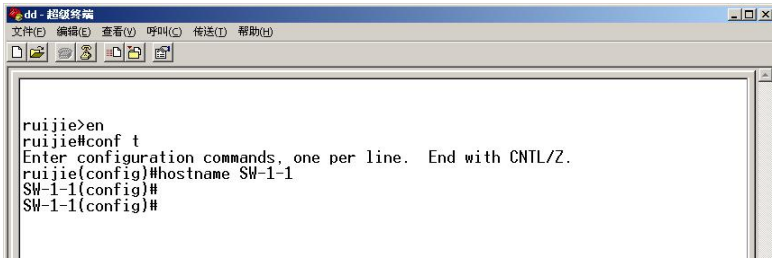


图 7-24 修改接入层交换机名称

（4）核心层与汇聚层交换机均为三层交换机，在核心层和汇聚层之间要运行路由协议，所以三层交换机要开启三层接口功能。

由于三层交换机端口默认为二层接口，所以需要用“no switchport”命令，启用三层路由功能后，才可以直接为端口配置 IP 地址（不同品牌的交换机设置不同，有的是通过 VLAN 设置 IP 地址的方式实现），如图 7-25 所示。

```
SW-HX>
SW-HX>en
SW-HX#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-HX(config)#int g0/25
SW-HX(config-if)#no switchport
SW-HX(config-if)#ip address 10.16.0.2 255.255.255.0
SW-HX(config-if)#no shut
SW-HX(config-if)#
```

图 7-25 给三层接口配置 IP 地址

3）具体接口及 IP 参数如表 7-1 所示。

表 7-1　接口 IP 地址分配表

设　备	接　口	IP 地址	子 网 掩 码
防火墙	GE2	202.181.111.85	255.255.255.0
	GE3	10.18.0.1	255.255.255.0
	GE4	10.16.0.1	255.255.255.0
核心交换机 SW-HX	GE0/25	10.16.0.2	255.255.255.0
	GE0/26	10.0.1.1	255.255.255.0
	GE0/27	10.0.2.1	255.255.255.0
	GE0/28	10.0.3.1	255.255.255.0
汇聚层交换机 SW-1-H	GE0/28	10.0.1.2	255.255.255.0
	GE0/27	10.0.4.1	255.255.255.0
汇聚层交换机 SW-2-H	GE0/28	10.0.2.2	255.255.255.0
	GE0/27	10.0.4.2	255.255.255.0
	GE0/26	10.0.5.1	255.255.255.0
汇聚层交换机 SW-3-H	GE0/28	10.0.3.2	255.255.255.0
	GE0/26	10.0.5.2	255.255.255.0

4）核心层、汇聚层交换机 IP 参数的设置如图 7-26 ~ 7-28 所示。

```
SW-HX(config)#int G0/25
SW-HX(config-if)#no switchport
SW-HX(config-if)#ip address 10.16.0.2 255.255.255.0
SW-HX(config-if)#no shutdown
SW-HX(config-if)#exit
SW-HX(config)#int G0/26
SW-HX(config-if)#no switchport
SW-HX(config-if)#ip address 10.0.1.1 255.255.255.0
SW-HX(config-if)#no shutdown
SW-HX(config-if)#exit
SW-HX(config)#int G0/27
SW-HX(config-if)#no switchport
SW-HX(config-if)#ip address 10.0.2.1 255.255.255.0
SW-HX(config-if)#no shutdown
SW-HX(config-if)#exit
SW-HX(config)#int G0/28
SW-HX(config-if)#no switchport
SW-HX(config-if)#ip address 10.0.3.1 255.255.255.0
SW-HX(config-if)#no shutdown
SW-HX(config-if)#exit
SW-HX(config)#
```

图 7-26　核心层交换机 IP 参数设置

```
Enter configuration commands, one per line.  End with CNTL/Z.
SW-1-H(config)#int G0/28
SW-1-H(config-if)#no switchport
SW-1-H(config-if)#ip address 10.0.1.2 255.255.255.0
SW-1-H(config-if)#no shutdown
SW-1-H(config-if)#exit
SW-1-H(config)#int G0/27
SW-1-H(config-if)#no switchport
SW-1-H(config-if)#ip address 10.0.4.1 255.255.255.0
SW-1-H(config-if)#no shutdown
SW-1-H(config-if)#exit
SW-1-H(config)#
```

图 7-27　1#楼汇聚层交换机 IP 参数设置

```
SW-2-H#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-2-H(config)#int
SW-2-H(config)#int  G0/28
SW-2-H(config-if)#no switchport
SW-2-H(config-if)#ip address 10.0.2.2 255.255.255.0
SW-2-H(config-if)#no shutdown
SW-2-H(config-if)#exit
SW-2-H(config)#int  G0/27
SW-2-H(config-if)#no switchport
SW-2-H(config-if)#ip address 10.0.4.2 255.255.255.0
SW-2-H(config-if)#no shutdown
SW-2-H(config-if)#exit
SW-2-H(config)#int  G0/26
SW-2-H(config-if)#no switchport
SW-2-H(config-if)#ip address 10.0.5.1 255.255.255.0
SW-2-H(config-if)#no shutdown
SW-2-H(config-if)#exit
```

图 7-28　2#楼汇聚层交换机 IP 参数设置

其他 3#楼与 1#楼汇聚层交换机 IP 参数设置类似，图略。

5）VLAN 规划及 IP 地址规划，见表 7-2。

表 7-2　VLAN 的 IP 地址表

建　筑　物	VLAN 编号	网 络 地 址	子 网 掩 码	路 由 聚 合
1#楼	101	10.1.1.0	255.255.255.0	10.1.0.0/16
	102	10.1.2.0	255.255.255.0	
	……	……	……	
2#楼	201	10.2.1.0	255.255.255.0	10.2.0.0/16
	202	10.2.2.0	255.255.255.0	
	……	……	……	
3#楼	301	10.3.1.0	255.255.255.0	10.3.0.0/16
	302	10.3.2.0	255.255.255.0	
	……	……	……	
继续扩展如 4#楼	401	10.4.1.0	255.255.255.0	10.4.0.0/16
	402	10.4.2.0	255.255.255.0	
	……	……	……	

6）VLAN 配置如图 7-29 和图 7-30 所示。

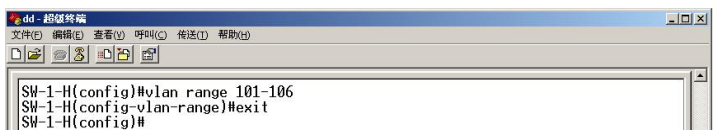


图 7-29　1#楼汇聚层交换机创建 VLAN

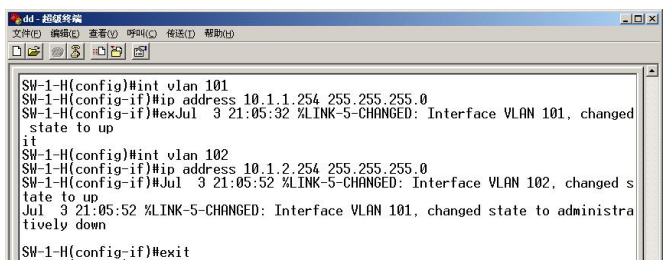


图 7-30　1#楼汇聚层交换机 VLAN 的 IP 设置

步骤二：硬件防火墙配置。

1）配置硬件防火墙各接口 IP 地址，点击“网络管理”→“接口”→“编辑”→输入相对应的 IP 地址，配置完成后如图 7-31 所示。

图 7-31　硬件防火墙各接口 IP 地址设置

2）配置缺省网关，点击“网络管理”→“基本配置”→“缺省网关”→“新建”→输入网关的地址，配置完成后如图 7-32 所示。

图 7-32　硬件防火墙缺省网关设置

3）配置 DNS，点击“网络管理”→“基本配置”→“DNS 配置”→输入 DNS 的地址，配置完成后如图 7-33 所示。

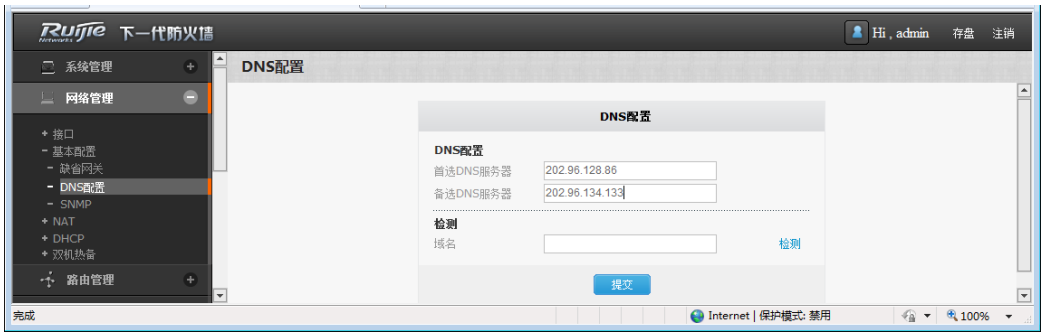


图 7-33　硬件防火墙 DNS 的配置

4）配置静态路由，点击“路由管理”→“静态路由”→“新建”→输入 IP 子网和掩码及下一跳地址，配置完成后如图 7-34 所示。

5）配置 NAT，点击“网络管理”→“NAT”→“NAT 规则”→“新建”→“源地址转换”→设置如图 7-35 所示参数，配置完成后如图 7-36 所示。

6）配置安全策略，点击“防火墙”→“安全策略”→“新建”→设置好源、目的、服务和动作参数，配置完成后如图 7-37 所示。

图 7-34　硬件防火墙的静态路由设置

图 7-35　硬件防火墙 NAT 中新建源地址转换

图 7-36　硬件防火墙 NAT 配置

图 7-37　硬件防火墙安全策略设置

7）配置安全防 DOS 攻击，单击“入侵防御”→“配置”→设置如图 7-38 所示的参数→

确定。

图 7-38　硬件防火墙安全防 DOS 攻击设置

步骤三：路由及 ACL 配置。

1）核心交换机静态路由及 ACL 设置，如图 7-39 和图 7-40 所示。

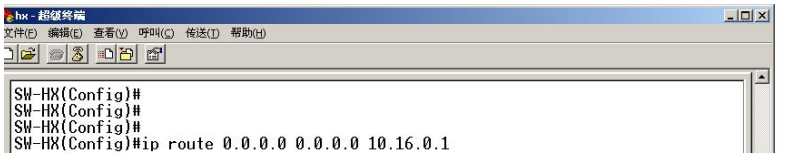


图 7-39　核心交换机静态路由配置

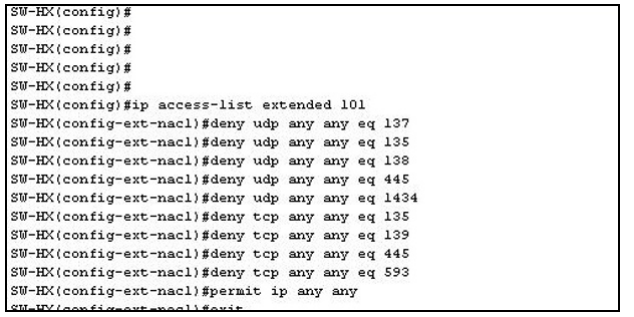


图 7-40　核心交换机 ACL 的配置

2）动态 OSPF 配置如图 7-41 和图 7-42 所示。

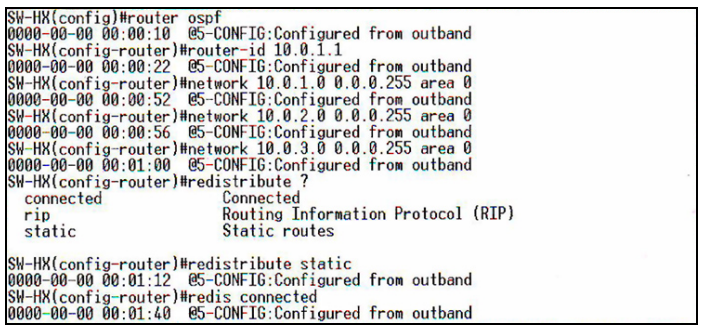


图 7-41　核心交换机 OSPF 配置

```
SW-HX(config)#router ospf
38144-00-112 248:176:00  @5-CONFIG:Configured from outband
SW-HX(config-router)#area 0 authentication message-digest
0000-00-00 00:00:11  @5-CONFIG:Configured from outband
SW-HX(config-router)#exit
0000-00-00 00:00:13  @5-CONFIG:Configured from outband
SW-HX(config)#int ra g 0/26-28
0000-00-00 00:00:26  @5-CONFIG:Configured from outband
SW-HX(config-if-range)#ip ospf message-digest-key 1 md5 net-2011
0000-00-00 00:00:42  @5-CONFIG:Configured from outband
SW-HX(config-if-range)#
```

图 7-42　核心交换机 OSPF 协议 MD5 认证配置

3）汇聚层交换机 SW-2-H、SW-3-H 的 OSPF 协议配置及 OSPF 协议 MD5 认证配置参照图 70-43 和图 7-44 所示配置。

```
!
end

SW-1-H#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-1-H(config)#no router ospf
@5-CONFIG:Configured from outband
SW-1-H(config)#router ospf
@5-CONFIG:Configured from outband
SW-1-H(config-router)#router-id 10.0.1.2
@5-CONFIG:Configured from outband
SW-1-H(config-router)#network 10.0.1.0 0.0.0.255 area 0
@5-CONFIG:Configured from outband
SW-1-H(config-router)#network 10.0.4.0 0.0.0.255 area 0
@5-CONFIG:Configured from outband
SW-1-H(config-router)#network 10.1.0.0 0.0.255.255 area 0
@5-CONFIG:Configured from outband
SW-1-H(config-router)#
```

图 7-43　汇聚层交换机 SW-1-H 上 OSPF 协议的设置

```
SW-1-H(config)#router ospf
38220-00-112 68:232:00  @5-CONFIG:Configured from outband
SW-1-H(config-router)#area 0 authentication message-digest
0000-00-00 00:00:31  @5-CONFIG:Configured from outband
SW-1-H(config-router)#area 1 authentication message-digest
0000-00-00 00:00:37  @5-CONFIG:Configured from outband
SW-1-H(config-router)#exit
0000-00-00 00:00:38  @5-CONFIG:Configured from outband
SW-1-H(config)#int ran g 0/27-28
0000-00-00 00:00:58  @5-CONFIG:Configured from outband
SW-1-H(config-if-range)#ip ospf message-digest-key 1 md5 net-2011
0000-00-00 00:01:26  @5-CONFIG:Configured from outband
SW-1-H(config-if-range)#
```

图 7-44　汇聚层交换机 SW-1-H 上 OSPF 协议的 MD5 认证配置

4）OSPF 协议的运行情况，如图 7-45 所示。

```
  Backup       - active,and there is at least one better route whose distance is
smaller.
                    For ECMP route,another possible reason is that it is learni
ng linklayer address of nexthop

Type Destination IP      Next hop         Interface Distance Metric   Status
---- ----------------- ---------------- --------- -------- -------- --------
S    0.0.0.0/0         10.16.0.1        Gi0/25    1        0        Active
C    10.0.1.0/24       0.0.0.0          Gi0/26    0        0        Active
C    10.0.2.0/24       0.0.0.0          Gi0/27    0        0        Active
C    10.0.3.0/24       0.0.0.0          Gi0/28    0        0        Active
O    10.0.4.0/24       10.0.1.2         Gi0/26    110      2        Active
O    10.0.5.0/24       10.0.2.2         Gi0/27    110      2        Active
O    10.1.1.0/24       10.0.1.2         Gi0/26    110      2        Active
O    10.1.2.0/24       10.0.1.2         Gi0/26    110      2        Active
O    10.2.1.0/24       10.0.2.2         Gi0/27    110      2        Active
O    10.2.2.0/24       10.0.2.2         Gi0/27    110      2        Active
O    10.3.0.0/16       10.0.3.2         Gi0/28    110      51       Active
C    10.16.0.0/24      0.0.0.0          Gi0/25    0        0        Active
```

图 7-45　核心交换机 SW-HX 上 OSPF 协议运行情况及路由信息

其他汇聚层交换机 SW-1-H、SW-2-H、SW-3-H 上的 OSPF 协议运行情况，可通过“show ip route”命令来显示，图略。

步骤五：配置链路聚合

（1）汇聚层交换机的配置与接入层交换机之间的双链路聚合，如图 7-46 所示。

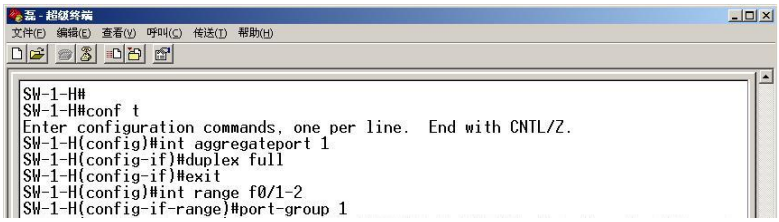


图 7-46　双链路聚合配置

（2）其他汇聚层交换机和接入层交换机的链路聚合参照图 7-46 所示进行配置，在接入层交换机与汇聚层交换机之间形成双链路，既扩展了带宽，实现了冗余，又能避免广播风暴。

项目测试

在企业的接入层 PC 接入测试到外网口 202.181.111.85 的连通性，如图 7-47 所示。

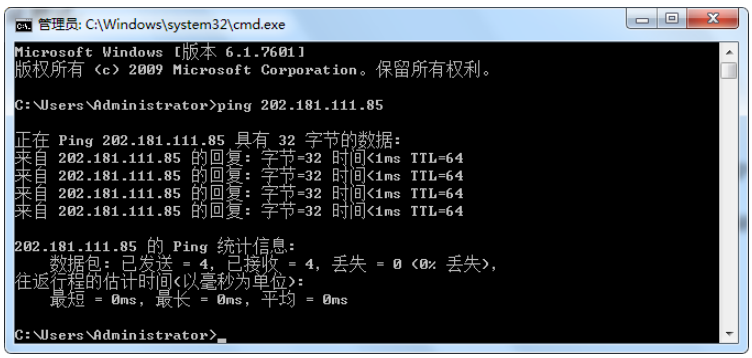


图 7-47　测试到外网口的连通性

认证测试

一、选择题

1．包过滤防火墙的缺点为（　　）。

A．容易受到 IP 欺骗攻击

B．处理数据包的速度较慢

C．开发比较困难

D．代理的服务（协议）必须在防火墙出厂之前进行设定

2．如果内部网络的地址网段为 192.168.1.0/24 ，需要用到防火墙的哪个功能，才能使用户上网（　　）。

A．地址映射　　B．地址转换

C．IP 地址和 MAC 地址绑定功能　　D．URL 过滤功能

3．防止盗用 IP 行为是利用防火墙的（　　）功能。

A．防御攻击的功能　　B．访问控制功能

C．IP 地址和 MAC 地址绑定功能　　D．URL 过滤功能

4．防火墙（　　）不通过它的连接。

A．不能控制　　B．能控制

C．能过滤　　D．能禁止

5．防火墙对数据包进行状态检测包过滤时，不可以进行过滤的是（　　）。

A．源和目的 IP 地址　　B．源和目的端口

C．IP 协议号　　D．数据包中的内容

6．当用户网络有多个公网出口时，需要用到防火墙的什么功能（　　）。

A．OSPF　　B．H.323　　C．DHCP　　D．PBR

7．防火墙对要保护的服务器作端口映射的好处是（　　）。

A．便于管理

B．提高防火墙的性能

C．提高服务器的利用率

D．隐藏服务器的网络结构，使服务器更加安全

8．下面关于防火墙的说法中，错误的是（　　）。

A．防火墙可以强化网络安全策略

B．防火墙可以防止内部信息外泄

C．防火墙能防止感染了病毒的软件或文件传输

D．防火墙可以限制网络暴露

二、简答题

1．简述什么是防火墙。

2．简述混合型防火墙的工作原理。

3．描述下一代防火墙与传统防火墙的区别。

4．描述下一代防火墙的主要功能。

5．简述配置下一代防火墙 NAT 的主要步骤。

附录 A

Cisco 命令汇总

命　令	描　述
?	给出一个帮助屏幕
access-class	将标准的 IP 访问控制列表应用到 VTY 线路
access-list	创建一个访问控制列表
any	指定任何主机或任何网络，作用与 0.0.0.255.255.255.255 命令相同
bandwidth bw	设置一个串行接口的带宽为 bw
banner motd	指定信息标语
boot system flash iosname	从 Flash 中的 iosname 启动，ISO 名为 isname
boot system room	从 ROM 中启动
boot system tftp iosname address	从 TFTP 服务器启动，IOS 名为 iosname
cdp enable	打开一个特定接口的 CDP
cdp holdtime	修改 CDP 的保持时间
cdp run	打开路由器上的 CDP
cdp timer	修改 CDP 更新定时器
channer-group channel-num mode	指定一个接口到以太通道，设置交换机的通道模式
clear counters	清除某一接口上的统计信息
clear ip nat translation *	从 NAT 转换表中清除所有的动态地址转换条目
clear ip route *	清除路由器的路由表
clear line	清除通过 Telnet 连接到路由器的连接
clear mac-address-table	清除该交换机动态创建的过滤表
clock rate	在串行 DCE 接口上设置时钟
clock set	设置路由器的时钟
connect	开启一个 Telnet 连接
config memory	复制 startup-config 到 running-config
config terminal	进入全局配置模式
config-register	告诉路由器如何启动以及修改配置寄存器的配置
copy flash tftp	将 ISO 复制到 TFTP 主机
copy running-config startup-config	将当前配置文件复制到 NVRAM 中
copy running-config tftp	将 running-config 文件复制到 TFTP 主机
copy startup-config tftp	把 NVRAM 中的配置文件复制到 TFTP 主机上
copy startup-config running-config	把 NVRAM 中的配置文件复制到 RAM 中
copy tftp flash	将 ISO 从 TFTP 复制到 Flash 中
copy tftp running-config	将配置文件从 TFTP 主机复制到 running-config 文件
copy tftp startup-config	将配置文件从 TFTP 主机复制到 NVRAM 中
debug dialer	显示呼叫建立和结束的过程
debug frame-relay lmi	显示在路由器和帧中继交换机之间的 lmi 交换信息
debug ip igrp events	提供在网络中运行的 IGRP 路由选择信息的概要

续表

命　令	描　述
debug ip igrp transactions	显示来自相邻路由器要求更新的请求消息和路由器发到相邻路由器的广播消息
debug ip rip	显示有关在路由器接口上收发 RIP 数据包的信息
debug isdn q921	显示 ISDN 第二层进程
debug isdn q931	显示 ISDN 第三层进程
delete vlan	删除 VLAN 数据库（此命令在使用时应非常注意）
description	在接口上设置一个描述
dialer idle-timeout number	指定 ISDN 的空闲时间
dialer list number protocolprotocol[permit|deny]	为 DDR 链路指定触发 DDR 的流量
dialer load-threshold number	设置什么时候在 ISDN 链路上启动第二条 BRI 的参数
dialer map protocol address name hostname number	代替拨号串，为 ISDN 网络中提供更好的安全性
dialer string	设置用于拨叫 BRI 接口的电话号码
disable	从特权模式返回用户模式
disconnect	断开同远程路由器的连接
distance	改变路由协议的管理距离
duplex	指定端口的工作方式，全双工还是半双工
enable	进入特权模式
enable password	设置从用户模式进入特权模式的密码，密码为明文
enable secret	设置从用户模式进入特权模式的密码，密码为密文
encapsulation	在接口上设置帧的封装类型
encapsulation encapsulationg dotlq vlan-num	VLAN 间路由时，在子接口上封装 Trunk 类型
erase startup-config	删除路由器上 NVRAM 的内容
exit	终止任何配置模式或关闭一个活动的会话
frame-relay interface-dlci	在串行链路或子接口上配置 PVC 地址
frame-relay lmi-type	在串行链路上配置 LMI 类型
frame-relay map protocol protocol-address dlci	帧中继静态映射
help	获得交互式帮助
history	查看历史记录
host	指定一个主机地址
hostname	设置一台路由器或交换机的名字
interface	进入接口配置模式
interface prot-channel channel-num	生成一个以太通道，并指定通道号码（1～6）
ip access-group	将 IP 访问列表应用到一个接口
ip address	设置一个接口或交换机 IP 地址
ip bandwidth-perecnt eigrp	配置 EIGRP 路由数据包占用的带宽百分比
ip classless	在路由器上启用无类别地址
ip default-gateway	设置默认网关
ip default-network	建立一条静态路由
ip domain-loopup	打开 DNS 查找功能（默认时打开）
ip domain-name	将域名添加到 DNS 查找名单中
ip hello-interval eigrp	配置 EIGRP 的 HELLO 数据包的发送时间间隔
ip hold-time eigrp	配置 EIGRP 的 HELLO 数据包的保持时间

续表

命　令	描　述
ip host	在路由器上创建主机表
ip name-server	设置 DNS 服务器的 IP 地址（最多 6 个）
ip nat{inside|outside}	指定 NAT 的内/外部接口
ip nat nside destination	建立一个动态 NAT 内部目的地地址转换
ip nat inside source	将内部本地地址与内部合法地址进行地址转换
ip nat pool name start-ip end-ip	定义一个可以根据需要进行分配的 NAT 全球地址池
ip ospf priority	配置接口的 OSPF 优先级
ip ospf cost	设置接口的 cost 值（OSPF)
ip ospf hello-interval	配置 OSPF 的 HELLO 数据包发送时间间隔
ip ospf dead-interval	配置 OSPF 判定邻居死机的时间间隔
ip route	在路由器上创建静态或默认路由
isde switch-type	设置 ISDN 交换机的交换类型
line	进入配置模式以修改和设置用户模式口令
line aux	进入辅助接口配置模式
line console 0	进入控制台配置模式
line vty	进入 VTY 接口配置模式
logging synchronous	阻止控制台信息覆盖命令行上的输入
logout	退出控制台会话
maximum-paths	配置到达同一网络的最大路径数
meric maximum-hop	配置路由的最大跳数
mertric weights 0 k1 k2　k3 k4 k5	改变 IGRP，EIGRP 的度量值计算因子
network	告诉路由选择协议要发通告的网络
no cdp enable	关闭接口上的 CDP
no ip domain-lookup	关闭 DNS 查找功能
no shutdown	打开一个接口
no vlan vlan-num	删除 VLAN
ospf auto-cost reference-bandwidth	配置 OSPF 计算 cost 的公式的分母
passive-interface	使接口不发送路由更新
ping	测试网络的连通性
ppp authentucation chap	告诉 PPP 使用 CHAP 认证方式
ppp authentucation pap	告诉 PPP 使用 PAP 认证方式
ppp chap hostname hostname	设置 chap 验证的主机名
ppp chap password password	设置 chap 验证的密码
ppp pap sent-username username password password	设置路由器取得对方 ppp 验证时的用户名和密码
reload	重启路由器
router-id	设置 OSPF 中路由器的 ID
router igrp	配置 IGRP 路由协议
router rip	配置 RIP 路由协议
router ospf	配置 OSPF 路由协议
secondary	在同一个物理接口上添加辅助 IP 地址
service password-encryption	对口令进行加密
setup	运行路由器初始配置
show access-list	显示路由器上配置的所有访问列表

续表

命　令	描　述
show arp	显示 ARP 缓存表
show buffers	提供有关路由器缓冲空间的统计信息
show cdp	显示 CDP 定时器和保持时间周期
show cdp entry*	同 show cdp neighbor detail 命令一样
show cdp interface	显示启用了 CDP 的特定接口信息
show cdp neighbor	显示直连的相邻设备及其详细信息
show cdp neighbor detail	显示 IP 地址和 IOS 版本和类型，并且包括 show cdp neighbor 命令显示所有信息
show cdp traffic	显示设备发送和接收的 CDP 分组数以及任何出错信息
show clock	显示路由器的时间
show controllers	显示接口的 DTE 或 DCE 状态
show dialer	显示接口在拨什么号码之类的信息
show flash	显示 Flash 的文件
show frame-relay map	显示静态的和动态的网络层到 PVC 的映射
show frame-relay pvc	显示路由器上已配置的 PVC 和 DLCI 号
show history	默认时显示最近输入的 10 个命令
show hsots	显示主机表中的内容
show interfacds	显示路由器上配置的所有接口的状态
show interfaces [int mode/port]switchport	显示交换机上的交换端口属性
show ip access-list	只显示 IP 访问列表
show ip eigrp neighbors	可以查看路由器的 EIGRP 邻居表
show ip eigrp topology	查看路由器的 EIGRP 拓扑表
show ip eigrp taffic	显示 EIGRP 的各种类型数据包统计
show ip interaces	列出接口的状态和全局参数
show ip nat statistics	显示 NAT 有关转换的统计信息
show ip nat translation[verbose]	显示活跃的 NAT 转换
show ip protocols	显示活跃的路由协议进程、参数和当前状态
show ip route	显示 IP 路由表
show ip ospf database	显示 OSPF 链路状态数据库
show ip ospf interface	显示路由器各接口的 OSPF 信息
show ip ospf neighbors	查看路由器的 OSPF 邻居表
show isde active	显示呼叫的号码和呼叫是否在进行中
show isde status	显示 ISDN 的状态
show memory	显示路由器内存的大小，包括空闲内存的大小
show process	显示路由器进程
show protocols	显示配置协议
show running-config	显示当前在该路由器上运行的配置
show sessions	显示通过 Telnet 到远程设备的连接
show stacks	显示监控和中断程序对堆栈的使用，并显示系统上一次重启的原因
show startup-config	显示保存在 NVRAM 中的备份配置
show version	显示系统的硬件配置、软件版本、配置文件的名称和来源及引导映像
show vlan {brief}	显示所有已配置的 VLAN
show vlan-membership	显示所有端口的 VLAN 分配

续表

命　令	描　述
show vtp {conters|status}	显示一台交换机的 VTP 配置
sutdown	设置接口为管理性关闭模式
switchport access vlan vlan-num	将交换机端口划到指定的 VLAN
switchport mode	指定交换端口模式、是 access 还是 trunk
switchport trunk encapsulation {dot1q|ISL}	指定交换机 trunk 端口的封装类型为 dotlq（）2950 系列无 ISL 封装
switchport trunk allowed vlan [add|removed] vlan-list	指定交换机 trunk 上允许增加或减少的 VLAN
telnet termainal eniting	开启一个 telnet 连接
termainal histrory size	改变历史记录的大小
termainal no editing	关闭高级编辑特性
timers basic	改变路由协议的各个定时器
trace	跟踪 IP 路由
traffic-share balanced	启用路由的负载均衡
traffic-share min	关闭路由的负载均衡，选择最佳路径
username name password password	为了 Cisco 路由器的身份验证创建用户名和口令
variance num	控制负载均衡最佳度量和最坏可接受度量之间的倍数
vlan database	进入 VLAN 配置模式
vlan vlan-num name vlan-name	创建一个 VLAN
vtp [server|client|transparence]	将该交换机设为一个 VTP 服务器、VTP 客户端或透明模式
vtp domain domain-name	设置 VTP 的域名
vtp password password	在该 VTP 域上设置一个口令
vtp pruning enable	使该交换机成为一台修剪交换机
write	运行的配置信息写入内存、网络或终端

附录 B

常见 TCP、UDP 端口号以及助记符

协　　议	助　记　符	意义及实际值
TCP	Bgp	Border Gateway Protocol (179)
	Chargen	Character generator (19)
	Cmd	Remote commands (rcmd, 514)
	Daytime	Daytime (13)
	Discard	Discard (9)
	Domain	Domain Name Service (53)
	Echo	Echo (7)
	Exec	Exec (rsh, 512)
	Finger	Finger (79)
	Ftp	File Transfer Protocol (21)
	Ftp-data	FTP data connections (20)
	Gopher	Gopher (70)
	Hostname	NIC hostname server (101)
	Irc	Internet Relay Chat (194)
	Klogin	Kerberos login (543)
	Kshell	Kerberos shell (544)
	Login	Login (rlogin, 513)
	Lpd	Printer service (515)
	Nntp	Network News Transport Protocol (119)
	Pop2	Post Office Protocol v2 (109)
	Pop3	Post Office Protocol v3 (110)
	Smtp	Simple Mail Transport Protocol (25)
	Sunrpc	Sun Remote Procedure Call (111)
	Syslog	Syslog (514)
	Tacacs	TAC Access Control System (49)
	Talk	Talk (517)
	Telnet	Telnet (23)
	Time	Time (37)
	Uucp	Unix-to-Unix Copy Program (540)
	Whois	Nicname (43)
	Www	World Wide Web (HTTP, 80)
UDP	biff	Mail notify (512)
	bootpc	Bootstrap Protocol Client (68)
	bootps	Bootstrap Protocol Server (67)
	discard	Discard (9)
	dns	Domain Name Service (53)
	dnsix	DNSIX Securit Attribute Token Map (90)

续表

协　　议	助　记　符	意义及实际值
UDP	Echo	Echo (7)
	mobilip-ag	MobileIP-Agent (434)
	mobilip-mn	MobilIP-MN (435)
	nameserver	Host Name Server (42)
	netbios-dgm	NETBIOS Datagram Service (138)
	netbios-ns	NETBIOS Name Service (137)
	netbios-ssn	NETBIOS Session Service (139)
	ntp	Network Time Protocol (123)
	rip	Routing Information Protocol (520)
	snmp	SNMP (161)
	snmptrap	SNMPTRAP (162)
	sunrpc	SUN Remote Procedure Call (111)
	syslog	Syslog (514)
	tacacs-ds	TACACS-Database Service (65)
	talk	Talk (517)
	tftp	Trivial File Transfer (69)
	time	Time (37)
	who	Who(513)
	Xdmcp	X Display Manager Control Protocol (177)